МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Поволжский государственный университет телекоммуникаций и информатики»

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

Диссертация на соискание ученой степени кандидата технических наук

Научный руководитель:

доктор технических наук, доцент

Шакурский Максим Викторович

Самара – 2026

ОГЛАВЛЕНИЕ

Введение 5

1. Анализ систем и методов сокрытия информации. Постановка задачи исследования 15

1.1. Классификация звуковых форматов 19

1.2. Обзор известных методов стеганографии для звуковых покрывающих объектов 27

1.3. Оценка маскировки информации 29

1.4. Характеристика атак на стегосистемы и описание модели нарушителя 33

Выводы по первой главе. Цель и задачи исследования 36

2. Математические модели подсистем встраивания сообщения в покрывающий объект из стеганографической системы 38

2.1. Математическая модель стеганографической системы использующей встраивание двух компонент в пределах одного отсчета с использованием функции исключающего ИЛИ 38

2.2. Математическая модель стеганографической системы использующей встраивание двух компонент в пределах окна фиксированного размера с использованием функции исключающего ИЛИ 45

2.3. Математическая модель стеганографической системы использующей встраивание двух компонент в пределах окна фиксированного размера с использованием условных функций определения второй компоненты стегоконтейнера 47

Выводы по второй главе 55

3. Методика анализа битовых последовательностей на основе NIST тестов 56

3.1. Анализ битовых последовательностей на основе NIST тестов 57

3.2. Модель сообщения 63

3.3. Методика оценки последовательностей 68

Выводы по третьей главе 87

4. Исследование свойств стеганографических систем 89

4.1. Исследование свойств покрывающих объектов 89

4.2. Исследование систем встраивания информации в пределах одного отсчета 94

4.2.1 Встраивание двух компонент в пределах одного отсчета с использованием функции исключающего ИЛИ 95

4.2.2 Многослойное встраивание двух компонент в пределах одного отсчета с использованием функции исключающего ИЛИ 107

4.3. Исследование систем встраивания информации в пределах окна фиксированного размера 111

4.3.1 Модель стеганографической системы использующей встраивание двух компонент в пределах окна фиксированного размера с использованием функции исключающего ИЛИ 112

4.3.2 Модель стеганографической системы, использующей встраивание двух компонент в пределах окна фиксированного размера с использованием условных функций определения второй компоненты стегоконтейнера 114

Выводы по четвертой главе 131

Заключение 133

Список литературы 135

Приложение 1. Акты внедрения результатов диссертационного исследования 150

Приложение 2. Полученные патенты и свидетельства о регистрации программ для ЭВМ и электронных ресурсов 154

Приложение 3. Результаты экспериментов 162

П 3.1 Тестирование музыкальных фрагментов при встраивании двух компонент в пределах одного отсчета с использованием функции исключающего ИЛИ..... 162

П3.2 Тестирование музыкальных фрагментов при многослойном встраивании двух компонент в пределах одного отсчета с использованием функции исключающего ИЛИ..... 178

Введение

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

Существующие стеганографические методы использования звуковых покрывающих объектов ориентированы либо на младшие битовые слои, обладающие известными статистическими свойствами, либо не учитывают изменения статистических характеристик старших битовых слоев. Кроме того, 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 разработанности темы диссертационного исследования. 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 удаленной 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.

Объект исследования – 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.

Цель 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 соелующие 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 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.

Полученные теоретические положения могут быть использованы при дальнейшем исследовании и моделировании систем скрытой передачи информации в цифровых медиаформатах, в том числе в режиме реального времени.

Практическая значимость исследования заключается в возможности 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 исследований 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 соответствуют 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.

Результаты работы регулярно докладывались и обсуждались на научных конференциях: 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).

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», АО «РЦЗИ «ФОРТ».

Публикации. По теме диссертации 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.

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. Диссертационная работа 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.

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 аудиосигналов в реальном времени, например, наличие задержки приводит к блочной обработке данных, что, с одной стороны, ограничивает способы встраивания, а с другой — создает предпосылки для использования быстрых алгоритмов анализа и адаптации. Проведена оценка эффективности традиционных статистических методов анализа, включая дивергенцию Кульбака–Лейблера и коэффициент корреляции Пирсона, применительно к выявлению изменений в битовых слоях звуковых покрывающих объектов. Указанные методы обладают недостаточной чувствительностью для обнаружения зависимостей между битовыми слоями и изменениями, вызванными стеганографическим встраиванием. В результате этого обоснована необходимость применения расширенного статистического анализа, основанного на модифицированных NIST-тестах, а также предложен новый подход к использованию двухкомпонентного стеганографического контейнера, учитывающего особенности блочной обработки звуковых сигналов.

Во второй главе разработаны математические модели двухкомпонентных стеганографических систем для звуковых покрывающих объектов:

- встраивания одного бита сообщения в пределах одного отсчета;
- встраивания последовательности бит сообщения в пределах окна фиксированного размера;
- многоуровневого встраивания информации в несколько битовых слоев звукового сигнала.

Для многоуровневого встраивания разработан адаптивный механизм 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.

В третьей главе рассмотрены вопросы представления скрываемого сообщения и анализа его маскировки в звуковых покрывающих объектах. Обоснован выбор модели сообщения, включающей незашифрованный поток бит, а также потоки бит, зашифрованные алгоритмами AES и «Кузнечик». Для формирования тестового сообщения использован реальный файл формата PDF, содержащий текстовую и графическую информацию. Проведен сравнительный анализ степени маскировки зашифрованных и незашифрованных сообщений в различных звуковых покрывающих объектах с использованием набора NIST-тестов для анализа битовых последовательностей. Обнаружение зашифрованных фрагментов в области младших битовых слоев звуковых сигналов без сжатия является затруднительным вследствие отсутствия выраженной корреляции между битовыми слоями. Сделан вывод о том, что применение совокупности NIST-тестов является более информативной альтернативой традиционному анализу распределений значений бит с использованием дивергенции Кульбака–Лейблера.

В четвертой главе проведено экспериментальное исследование и численное моделирование разработанных стеганографических алгоритмов. Численное моделирование реализовано в среде Python для всех разработанных алгоритмов встраивания, включая и многоуровневое встраивание, а также варианты с адаптацией и без адаптации к статистическим свойствам покрывающего объекта. Разработанные алгоритмы зарегистрированы в виде программ ЭВМ. Проведены эксперименты для различных типов звуковых покрывающих объектов и сообщений, представленных в зашифрованном и незашифрованном виде. Экспериментально подтверждена корректность теоретических моделей и показано, что использование адаптивного

многоуровневого встраивания обеспечивает улучшенную маскировку информации, особенно в старших битовых слоях звукового сигнала.

В заключении диссертации приведены основные выводы и результаты выполненной работы.

В приложениях содержатся листинги компьютерных моделей, полученные по результатам работы патенты, а также материалы внедрения результатов диссертационной работы.

1. Анализ систем и методов сокрытия информации. Постановка задачи исследования

Стеганография — наука о скрытой передаче информации [17,20]. Стеганография, как маскировка или сокрытие информации существует уже тысячи лет, но ее современная форма – цифровая стеганография, получила интенсивное развитие в конце 1990-х годов, и в XXI столетии [8]. Это можно увидеть по количеству публикаций в базе цитирования Scopus, представленном на рисунке 1.1.

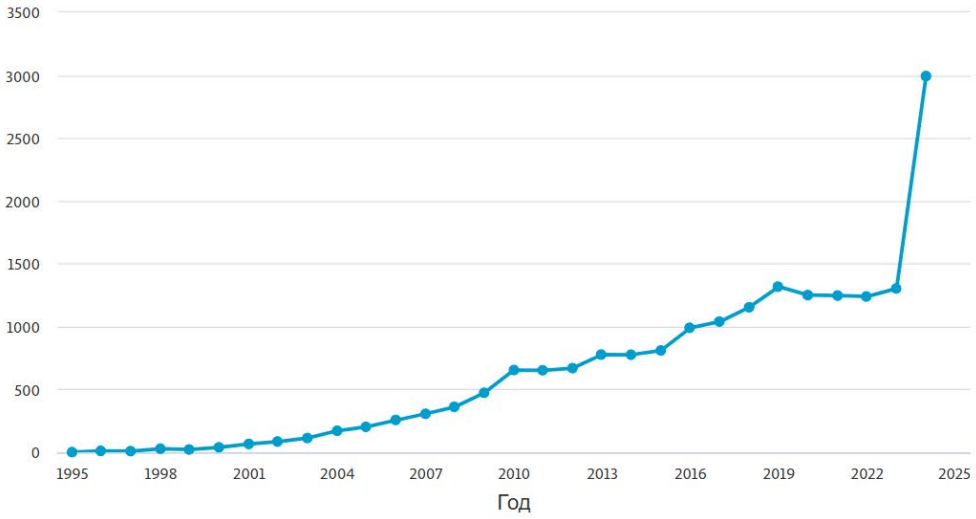


Рисунок 1.1 – Количество публикаций в базе Scopus по ключевому слову «steganography»

Стеганография, как направление, часто сравнивается с криптографией [18,25,50]. Дело в том, что данные направления, имеют много общего. Криптография и стеганография, дословно означают тайнопись. Оба направления преследуют цель обеспечения конфиденциальности передаваемых данных, методы в обоих направлениях могут иметь или не иметь ключ и т.д. Однако, при детальном рассмотрении эти направления имеют много отличий, особенно в области методов и областей применения. Более того, методы этих направлений могут применяться совместно.

Рассмотрим ключевые отличия стеганографии от криптографии.

Основное отличие заключается в целях шифрования. Криптография преследует цель защиты данных от прочтения в то время, как стеганография скрывает факт передачи сообщения. То есть, при установке скрытой коммуникации, передается открытая информация так, что злоумышленник ее может посмотреть и проанализировать, но внутри передаваемой информации скрываются сообщения, представляющие интерес. Если криптография гарантирует стойкое шифрование, то стеганография основывается на гипотезе, что злоумышленник пропустит скрытые сообщения. Сейчас основным средством обеспечения конфиденциальности информации является криптография. Это объясняется поддержкой криптографии на законодательном уровне, широким применением компьютерных сетей, интенсивным обменом информации и наличием большого количества протоколов, поддерживающих криптографическое шифрование. Однако в случае, если злоумышленник может воздействовать на передаваемую информацию, вплоть до ее разрушения, или даже разрушить канал передачи, то криптография не сможет обеспечить целостность сообщения. Тогда может использоваться стеганографическое сокрытие либо совместное применение криптографии и стеганографии. Например, в условиях, когда криптография запрещена на законодательном уровне (или криптографические ключи известны злоумышленнику) криптография не позволяет обеспечить конфиденциальность сообщений. Другой пример – связь в боевых условиях, когда каждая из сторон заинтересована в прослушивании или разрушении канала связи противника, при этом, сохраняя свои каналы связи.

Второе ключевое отличие заключается в том, что в криптографии нет требований к каналу. Есть шифруемые данные, в виде последовательности бит, к которым применяется шифрование (как правило блочное – AES, Кузнечик). Результатом шифрования является последовательность бит, которую злоумышленник не способен дешифровать, не имея ключа. В случае применения стеганографии, задачей становится маскировка сообщения внутри объекта, не вызывающего подозрение. То есть, набор методов встраивания информации определяется объектом (покрывающий объект – ПО), внутри которого спрятано

ценное сообщение. Таким образом, исследование стеганографии – это, в первую очередь, исследование ПО, а уже потом исследование методов [21,45].

Третье ключевое отличие заключается в принципе Керкгоффса – для криптографии он имеет основополагающее значение. В криптографии у злоумышленника может оказаться и фрагмент зашифрованного текста и, соответствующий ему фрагмент расшифрованного текста, но даже это не позволит ему вычислить ключ шифрования в ближайшем будущем. В случае стеганографии, если у злоумышленника будет оригинал ПО и ПО с встроенной информацией (стегосистема), то сравнивая побитно эти объекты он легко обнаружит отличия и предотвратит пересылку или всего контейнера, или разрушит встроенное сообщение.

Четвертое отличие заключается в методах шифрования (встраивания) информации и в методах оценки стойкости систем [38].

И, наконец, пятое отличие – в средствах. В криптографии для защищенной передачи информации по открытым каналам используются средства обмена ключами (алгоритмы с открытым ключом), средства шифрования (алгоритмы с закрытым ключом) и средства хэширования. В стеганографии два основных средства – средства скрытой передачи информации (стеганография или маскировка информации) и средства устойчивого маркирования объектов (цифровые водяные знаки) – неотделимые встройки в объект, обеспечивающие защиту авторских прав или передачу дополнительной информации (могут обнаруживаться сравнительно легко, но их разрушение крайне сложно).

Таким образом, можно утверждать, что стеганография – это отдельное научное направление, обладающее своими методами и средствами [13,14]. Заметим, что стеганография целиком привязана к типу ПО. Так, большинство работ данного направления фокусируют свое внимание на встраивании информации в изображения [72,92]. Это можно увидеть из рисунка 1.2, на котором приведен результат поиска по базе цитирования Scopus, используя ключевые слова «steganography» и «image».

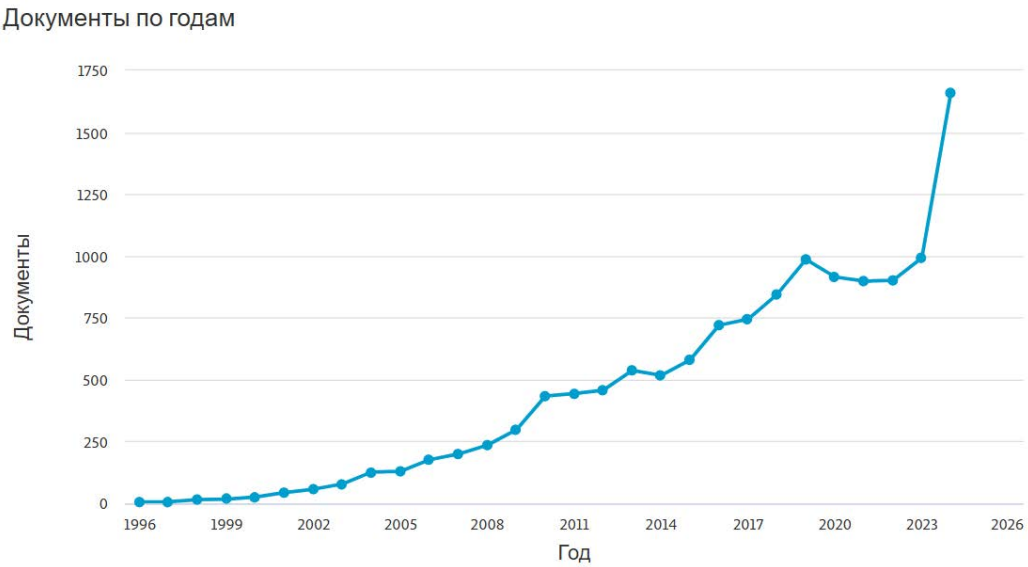


Рисунок 1.2 – Количество публикаций в базе Scopus по ключевому слову «steganography» и «image»

Исследования для изображений [52,70,72] объясняются сравнительной простотой их формирования и высокой визуальной наглядностью результатов. Еще одной причиной популярности данного типа ПО является его распространение в сетях передачи информации. Однако, развитие мессенджеров, социальных сетей и средств онлайн коммуникаций привело к распространению звуковых ПО. Наиболее сильный толчок для массового использования средств онлайн коммуникаций произошел в результате пандемии коронавируса, начавшейся в 2020 году. При этом исследования по стеганографии в звуке крайне ограничены, что можно увидеть на рисунке 1.3 [22]. Дело в том, что звуковые форматы сложнее в исследовании, а визуализация крайне сложна (особенно при наличии сжатия звука). Встраивание информации в звуковой поток в реальном времени представляет собой еще более сложную задачу, так как звуковые кодеки имеют высокую степень сжатия и, как следствие, минимальную информационную избыточность, что сильно ограничивает возможности стеганографии [15-16,47-48,78,103]. На рисунке 1.4 показан анализ публикационной активности в базе цитирования Scopus, используя ключевые слова «steganography» и «real time» (реальное время).

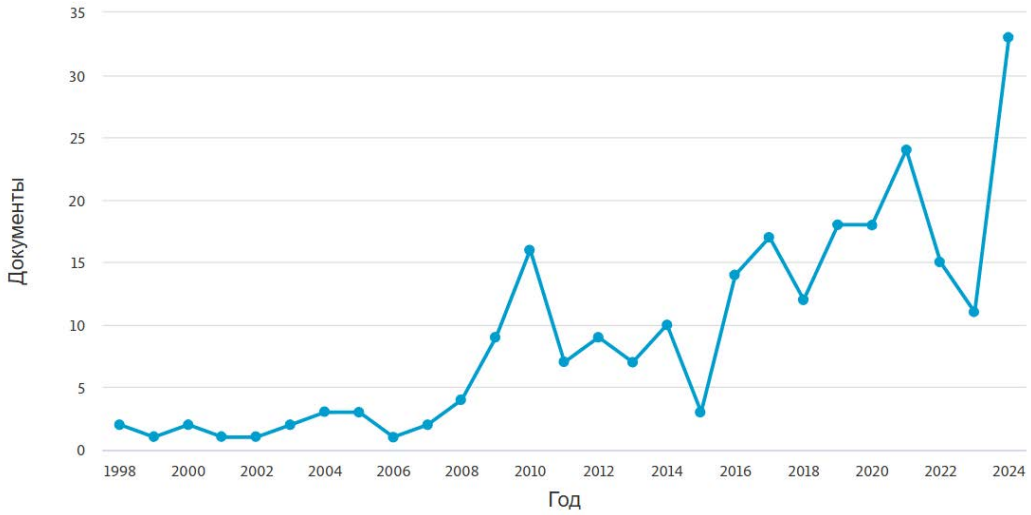


Рисунок 1.3 – Количество публикаций в базе Scopus по ключевому слову «steganography» и «sound»

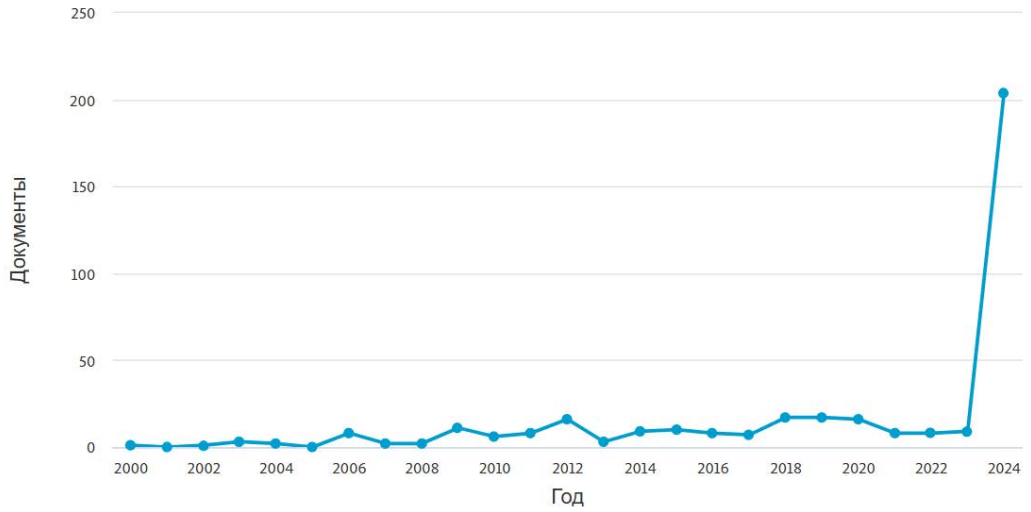


Рисунок 1.4 – Количество публикаций в базе Scopus по ключевому слову «steganography» и «real time»

Таким образом, можно сделать вывод, что исследование звуковых ПО является актуальной научной задачей. Рассмотрим основные звуковые форматы.

1.1. Классификация звуковых форматов

Звуковые форматы играют ключевую роль в современном мире мультимедиа. Они определяют, как звук кодируется, хранится и передается, что, в свою очередь, влияет на качество воспроизведения и совместимость с

различными устройствами. Рассмотрим основные категории звуковых форматов, их характеристики и области применения.

Звуковые форматы можно классифицировать по нескольким критериям: по способу сжатия, по количеству каналов, по типу хранения и по области применения.

По способу сжатия звуковые форматы делятся на два основных типа:

1. Без сжатия информации.
2. Со сжатием информации.

Форматы со сжатием информации в свою очередь делятся на:

– Форматы, использующие сжатие без потерь.

– Форматы, использующие сжатие с потерями.

Рассмотрим каждый тип формата подробнее.

Форматы без сжатия (например, WAV, AIFF) играют важную роль в обеспечении высокого качества звука [106]. Они сохраняют оригинальные звуковые данные, не прибегая к компрессии, что позволяет воспроизводить звук с максимальной точностью, обеспечивая высокое качество звука и не требующие значительного объема памяти. Такие форматы часто используются в профессиональной звукозаписи и редактировании. Данные форматы основаны на импульсно-кодовой модуляции.

Импульсно-кодовая модуляция (PCM) – это метод цифровой записи аналогового сигнала. PCM преобразует аналоговые звуковые волны в цифровую форму, фиксируя амплитуду сигнала в определенные моменты времени. Этот процесс включает два ключевых аспекта: дискретизацию и квантование. Квантование отвечает за количество бит, выделяемых на каждый отсчет, а дискретизация отвечает за частоту следования импульсов во времени. Более высокая частота дискретизации обеспечивает более точное воспроизведение звука.

Импульсно-кодовая модуляция и понятие частоты дискретизации являются основополагающими для понимания процесса преобразования аналогового звука в цифровую форму. Частота дискретизации указывает, сколько раз в секунду

происходит замер аналогового сигнала. Например, стандартная частота дискретизации для CD составляет 44,1 кГц, что означает, что сигнал измеряется 44 100 раз в секунду. Более высокие частоты, такие как 96 кГц или 192 кГц, используются в профессиональной аудиозаписи для достижения наилучшего качества звука.

Структура файла без сжатия обычно включает несколько основных компонентов:

1. Заголовок содержит информацию о формате файла, например, тип кодека, частоту дискретизации и количество каналов.

2. Аудиоданные – основная часть файла, где хранятся цифровые значения амплитуды сигнала.

3. Метаданные: Дополнительная информация о треке, такая как название песни, исполнитель и другие атрибуты.

Наиболее распространенными форматами без сжатия являются WAVE, AIFF.

Формат WAVE (Waveform Audio File Format) был разработан компанией Microsoft и является одним из самых популярных для хранения аудиоданных. WAVE-файлы могут содержать различные кодеки, однако чаще всего используют импульсно-кодовую модуляцию [23,73,76].

Формат AIFF (Audio Interchange File Format) разработан компанией Apple. AIFF также является форматом без сжатия, который часто используется в профессиональной аудиозаписи. AIFF-файлы сохраняют звук в высоком качестве и поддерживают метаданные.

Форматы со сжатием без потерь (например, FLAC, ALAC) представляют собой идеальное решение для тех, кто стремится сохранить высокое качество звука при уменьшении объема файлов. Принципы их работы основаны на эффективном удалении избыточности и использовании предсказательных моделей.

Сжатие без потерь основывается на алгоритмах, которые уменьшают размер файла, не теряя при этом информации.

Основные принципы работы форматов:

– Удаление избыточности: Многие звуковые данные содержат повторяющиеся элементы. Алгоритмы сжатия анализируют аудиосигнал и устраняют дублирующиеся данные, сохраняя только уникальные фрагменты.

– Предсказание: Некоторые форматы используют предсказательные модели для определения значений амплитуды на основе предыдущих значений. Это позволяет эффективно кодировать информацию, сохраняя только отклонения от предсказанных значений.

– Кодирование переменной длины: Использование кодов переменной длины позволяет более эффективно представлять часто встречающиеся значения. Например, более короткие коды могут использоваться для часто встречающихся амплитуд, в то время как редкие значения могут быть закодированы длинными последовательностями.

Структура файлов со сжатием без потерь включает несколько ключевых компонентов:

1. Заголовок содержит информацию о формате файла, включая тип кодека, частоту дискретизации, количество каналов и другие метаданные.

2. Данные аудио – это основная часть файла, где хранятся закодированные данные звука в виде последовательности битов, которые можно декодировать для воспроизведения.

3. Метаданные – это дополнительная информация о треке, которая позволяет пользователям легко идентифицировать аудиофайл и управлять им.

Наиболее распространенными форматами со сжатием без потерь являются FLAC, ALAC.

Формат FLAC (Free Lossless Audio Codec) один из самых распространенных форматов, который позволяет сжимать аудиофайлы без потерь и сохраняет оригинальное качество звука и поддерживает различные метаданные.

Формат ALAC (Apple Lossless Audio Codec) разработан компанией Apple и предлагает аналогичные преимущества FLAC, но оптимизирован для

использования в экосистеме Apple. Этот формат также обеспечивает высокое качество звука и совместимость с устройствами Apple.

Форматы со сжатием без потерь имеют достоинства и недостатки.

К основным достоинства можно отнести:

– Высокое качество звука. Сжатие без потерь гарантирует сохранение оригинального качества аудио.

– Меньший размер файлов. По сравнению с несжатыми форматами (например, WAV), файлы со сжатием без потерь занимают значительно меньше места на диске.

Однако есть и недостатки:

– больший размер по сравнению с форматами с потерями: Хотя файлы со сжатием без потерь меньше несжатых, они все же занимают больше места, чем форматы с потерями (например, MP3 или AAC).

Форматы со сжатием с потерями (например, MP3, AAC) – удаляют часть данных для уменьшения размера файла, что негативно сказывается на качестве звука. Сжатие аудиофайлов с потерями — это метод позволяет значительно уменьшить размер файлов за счет удаления некоторых данных, которые воспринимаются как менее важные для слуха. Эти форматы широко используются в потоковом аудио, мобильных устройствах и для хранения музыки.

В определении качества звука ключевую роль играет битрейт. Битрейт – это количество данных, передаваемых за единицу времени, измеряемое в килобитах в секунду (кбит/с).

Различают разные уровни битрейта:

– низкий битрейт (например, 64 кбит/с) – звук звучит плоско и нечетко.

– средний битрейт (128-192 кбит/с) – приемлемое качество для большинства слушателей, особенно в условиях обычного прослушивания.

– высокий битрейт (256-320 кбит/с) – максимальное качество для форматов с потерями, близкое к качеству CD.

Структура файлов со сжатием с потерями может отличаться в зависимости от формата, но обычно включает следующие элементы:

1. Заголовок содержит информацию о формате аудиофайла, включая тип кодека, частоту дискретизации и количество каналов (например, заголовок MP3 указывает на битрейт и версию MPEG).

2. Данные аудио являются основной частью файла, где хранятся закодированные данные звука, здесь аудиосигнал представлен в виде последовательности битов, которые декодируются при воспроизведении.

3. Метаданные – дополнительная информация (например, название песни, исполнитель, альбом и другие атрибуты), которая помогает пользователям идентифицировать файлы и управлять ими.

Достоинствами и недостатками форматов со сжатием с потерями являются:

Достоинства:

– меньший размер файлов. Эти форматы экономят место на диске и упрощают потоковую передачу.

– широкая совместимость. Большинство устройств и программ поддерживают форматы с потерями, такие как MP3 и AAC.

Недостатки:

– Потеря качества. При сжатии теряются некоторые детали звука, что может быть заметно для аудиофилов.

– Необратимость. В отличие от форматов без потерь, восстановить оригинальный звук после сжатия невозможно.

Основными форматами со сжатием с потерями являются:

Формат MP3 (MPEG Audio Layer III) один из самых популярных форматов для сжатия аудио, который использует алгоритмы, где удаляются звуковые данные, которые не могут быть восприняты человеческим ухом. Битрейт MP3 может варьироваться от 32 до 320 кбит/с, где более высокие значения обеспечивают лучшее качество звука [89].

Формат AAC (Advanced Audio Codec), разработанный как преемник MP3 и предлагает лучшее качество звука при том же битрейте. AAC используется в

таких платформах, как Apple Music и YouTube. Битрейт AAC обычно составляет от 64 до 256 кбит/с.

Формат OGG Vorbis – открытый формат, который обеспечивает отличное качество звука при низких битрейтах. OGG Vorbis часто используется в играх и на некоторых потоковых сервисах. Битрейт может варьироваться от 40 до 500 кбит/с.

Формат WMA (Windows Media Audio), разработанный Microsoft, который предлагает различные профили сжатия, включая WMA Standard и WMA Pro. Битрейт WMA может быть в диапазоне от 48 до 192 кбит/с для стандартного профиля.

Таблица 1.1 – Типовые аудиоформаты

Формат файла	Характеристики
Аудиоформаты без сжатия	
WAVE, WAV (Waveform Audio File Format) — формат файла-контейнера для хранения записи оцифрованного аудиопотока	Стандартный формат с дискретизацией 16 бит/44,1 кГц, применяемый во всех CD. Отличное качество воспроизведения из-за отсутствия сжатия и изменений, но размер файлов достигает очень больших размеров. Слабая поддержка метаданных (обложек, названий песен, и исполнителей). Достоинства: - высокое качество звука без потерь. - простота редактирования в аудиоредакторах. Недостатки: - большой размер файлов, что ограничивает объем хранения.
AIFF (Audio Interchange File Format) – формат аудиофайлов, применяемый для хранения звуковых данных на компьютерах и других электронных устройствах	Формат, разработанный компанией Apple на основе файлового формата (IFF). Файлы данного формата не сжимаются, в результате чего имеют большие размеры. Одна минута файла AIFF соответствует 44,1 кГц, 16 бит.
DSD (Direct Stream Digital) — однобитный аудиоформат, разработанный компаниями Sony и Philips, в котором используется кодирование плотностно-импульсной модуляцией	Применяется данный формат в Super Audio CD. Существует в вариантах с частотой дискретизации 2,8 МГц, 5,6 МГЦ. Формат не нашел широкого распространения и применения.

Аудиоформаты со сжатием без потерь	
APE – формат аудиофайлов, которые сжимаются кодеком Monkey’s Audio без потери качества	Расширение файла APE занимает значительно больше места на диске. Очень высокая степень сжатия аудиоданных. Данный формат поддерживает возможность исправления различных ошибок при записи, а также добавление тегов.
FLAC (Free Lossless Audio Codec) — свободный кодек, предназначенный для сжатия аудиоданных без потерь.	Формат со сжатием без потерь с поддержкой частот дискретизации, который позволяет уменьшить размер файла без потери качества звука. Достоинства: - сжатие без потерь, что сохраняет оригинальное качество. - поддержка метаданных. Недостатки: - меньшая совместимость по сравнению с форматами с потерями.
ALAC (Apple Lossless Audio Codec) — открытый аудиокодек для сжатия без потерь качества (lossless) цифровой музыки, разработанный Apple.	Собственный формат Apple со сжатием без потерь для Hi-Res, хранит в себе метаданные и значительно меньше по объему занимаемой информации по сравнению с WAV. Является альтернативой FLAC для iTunes.
Аудиоформаты со сжатием с потерями	
MP3	Популярный формат со сжатием с малым размером файла, качество звучания не высокое. Применяется для хранения музыки на смартфонах. MP3 использует метод психоакустического моделирования, чтобы удалить звуки, которые человеческое ухо не может воспринимать. Битрейт MP3 варьируется от 32 до 320 кбит/с, что позволяет пользователям выбирать между качеством звука и размером файла. Достоинства: - широкая совместимость с устройствами и программами. - возможность выбора битрейта в зависимости от потребностей пользователя.

	Недостатки: - потеря качества звука при низком битрейте. - невозможность восстановления оригинального звука после сжатия.
AAC (Advanced Audio Coding) — проприетарный (патентованный) формат аудиофайла с потерями.	Формат со сжатием и с потерями, как и MP3, но звучание лучше. Используется для скачивания с iTunes и трансляции с Apple Music (с битрейтом от 64 до 256 кбит/с) и трансляцией с YouTube. Достоинства: - более эффективное сжатие по сравнению с MP3. - поддержка многоканального звука. Недостатки: - меньшая совместимость с некоторыми старыми устройствами по сравнению с MP3.

1.2. Обзор известных методов стеганографии для звуковых покрывающих объектов

Стеганографические методы в звуке играют важную роль в обеспечении защиты авторских прав и управления цифровыми данными [12]. Современные методы маркирования, учитывающие различные способы преобразования информации, а также создание, внедрение и восстановление маркеров, опираются на следующие подходы: «расширение спектра», «лоскут», «добавление эхо», «изменение наименее значимых битов», «отпечатки пальцев» и «квантованная индексная модуляция». Рассмотрим каждый из перечисленных подходов более подробно:

Метод расширения спектра (spread spectrum) основан на идее распределения информационного сигнала по большей ширине частотного диапазона. Это достигается за счет модуляции аудиосигнала с использованием кодов, которые расщепляют сигнал на множество отдельных компонентов. Такой подход позволяет скрыть данные в аудиосигнале, минимизируя вероятность их обнаружения. Даже если часть сигнала будет потеряна или искажена, оставшиеся

компоненты все равно могут быть использованы для восстановления информации, что делает метод довольно устойчивым к различным видам атак.

Технология «лоскута» подразумевает вставку или замену небольших фрагментов аудиосигнала для внедрения маркера. Этот метод особенно полезен для реализации простых маркеров, не требующих больших объемов информации. Такие вставки могут быть сделаны в несущественных частях звуковой дорожки, что делает их менее заметными для обычного слуха. Однако стоит отметить, что этот подход может быть менее устойчивым к манипуляциям, поскольку злоумышленник может легко обнаружить и удалить такие маркеры.

Метод добавления эхо включает в себя создание задержки в сигнале с целью внедрения информации. В этом случае практически незаметное повторение звука (эхо) используется для кодирования данных. Данный подход может быть весьма эффективен, так как эхо, находящееся на грани восприятия, может быть закодировано так, что обычный слух не обнаружит вмешательства. Восстановление информации осуществляется за счет анализа временных характеристик эха, что делает этот метод достаточно интересным для исследования.

Метод «изменения наименее значимых битов» (LSB) является одним из самых распространенных методов стеганографии [6,51,54-57,60-66,71,74,81-83,86,88,91,93,95-96,99-100,104,107]. Он заключается в модификации последних битов цифрового аудиосигнала, что позволяет внедрять скрытые сообщения без заметного воздействия на общее качество звука. При этом изменения не воспринимаются человеческим ухом, так как они необычайно малы. Тем не менее, метод LSB может быть уязвим к атакам, например, при сжатии или конвертации аудиофайлов, что может повредить скрытую информацию.

Метод создания отпечатков пальцев акцентирует внимание на идентификации аудиосигналов на основе их уникальных характеристик. Это своего рода кодирование данных в характерных для аудиозаписи особенностях, например, в ритмическом рисунке или в специфических гармониках. Отпечатки пальцев позволяют не только маркировать аудиосигнал, но и отслеживать его

использование в сети, что также помогает в правозащитной деятельности. Такой подход требует более тщательной обработки сигнала, но обеспечивает высокую степень защищенности.

Квантованная индексная модуляция (QIM) – это метод, который сочетает в себе как элементы модуляции, так и квантования. Сигнал разбивается на участки, после чего для каждого из них выбирается индекс, который соответствует конкретному маркеру. Это позволяет внедрять маркировку, не искажая значимо аудиосигнал и сохраняя его качество. QIM обладает высокой стойкостью к атакам, так как изменение некоторых частей сигнала не приводит к его полной порче и позволяет восстановить внедренную информацию даже при наличии потерь. Применение подобных подходов в совокупности с вейвлет-преобразованием для повышения скрытности рассматривается в [94], а вопросы устойчивости встраиваемых данных к операциям переквантования более детально изучены в [97].

1.3. Оценка маскировки информации

Разработка стеганографических систем сопряжена с необходимостью оценки эффективности маскировки [37]. Стегоаналитик не должен иметь возможность сделать предположение о наличии скрытого сообщения с вероятностью выше 50%. При этом инструментарий, с помощью которого стегоаналитик выполняет проверку стеганографической системы, нам не известен. Поэтому задача маскировки заключается в разработке системы, максимально незаметной при любом инструменте проверки, что обеспечит невозможность определения наличия скрытого сообщения при комплексном применении средств стеганографического анализа (СА) [85].

В работах [1,6,24,35,40] рассматривается интересный подход к СА, основанный на использовании NIST тестов [53]. NIST тесты призваны показать, является ли битовая последовательность случайной. Идея применения тестов заключается в том, что к слоям изображения, представленным в виде битовых последовательностей, применяются NIST тесты, после чего анализируется

количество пройденных тестов. Результат сравнивается с ожидаемым для того или иного битового слоя.

В работе предлагается использование статистического аппарата NIST тестов для оценки маскировки информации стеганографическим алгоритмом. Рассмотрим состав NIST тестов.

Тестирование случайности является важным аспектом в области криптографии, компьютерной безопасности и статистического анализа. Стандартные тесты, разработанные Национальным институтом стандартов и технологий (NIST), предоставляют критически важные инструменты для оценки свойств случайных битовых последовательностей. NIST разработал набор из 15 тестов для оценки криптографических псевдослучайных числовых генераторов (ПСЧ). Эти тесты направлены на оценку статистических свойств выходных данных генераторов и их способности обеспечивать высокий уровень случайности. Рассмотрим состав тестов с точки зрения выявления скрытых последовательностей.

Частотный побитовый тест (Monobit test):

Суть этого теста – определить, равномерно ли распределены единицы и нули в битовой последовательности. Он подсчитывает количество единиц и сравнивает это значение с ожидаемым при случайном распределении. Цель – выявить отклонения от равновесия. Если количество единиц значительно отличается от числа нулей, это может сигнализировать о наличии закономерностей в данных. Присутствие таких закономерностей в младших битовых слоях может свидетельствовать о наличии скрытой информации.

Частотный блочный тест (Block frequency test):

Тест разбивает последовательность на фиксированные блоки и рассчитывает частоту единиц в каждом блоке. Затем результаты анализируются для выявления аномалий. Целью теста является – оценить устойчивость блочных структур к передаче скрытой информации. Если в некотором блоке частота единиц отличается от остальных, это может указывать на модификацию данных в пределах того или иного блока.

Тест на последовательность одинаковых битов (Runs Test):

Анализирует длину последовательностей одинаковых битов и их частоты. Помогает обнаружить скрытые зависимости, гарантируя, что не будет длинных последовательностей одинаковых бит. Происходит добавление метрик для анализа степени однородности пробегов и их вариабельности между разными участками последовательности может выявить скрытые зависимости.

Тест на самую длинную последовательность единиц в блоке (Longest Run of Ones Test):

Суть теста – анализ максимальной длины последовательности одинаковых бит (в основном единиц) в последовательности. Цель – определить наличие избыточной последовательности, что может быть связано с манипуляциями. Долгие последовательности единиц могут указывать на целенаправленную модификацию данных для сокрытия информации.

Тест рангов бинарных матриц (The binary matrix rank test):

Этот тест создает бинарную матрицу из данных и анализирует ее ранг и ранг отдельных блоков и строк. Целью является – выявление структурных аномалий в данных. Меньший ранг, чем ожидается, может сигнализировать о скрытии информации.

Спектральный тест (Discrete Fourier Transform Test):

Использует быстрое преобразование Фурье для анализа частотного спектра выходных данных для выявления периодичности. Ожидается, что спектр будет равномерно распределен (идентификация синусоидальных компонент); проявление явной периодичности указывает на слабости и попытки вставки данных.

Тест на совпадение неперекрывающихся шаблонов (Non-overlapping Template Matching Test):

Оценивает частоту появления заданных шаблонов в последовательности. Цель – проверить, насколько хорошо данные соответствуют заданной случайной модели. Отклонения показывают наличие структуры, что может быть признаком встраивания незашифрованной информации.

Тест на совпадение перекрывающихся шаблонов (Overlapping Template Matching Test):

Схож с предыдущим, но учитывает наложения шаблонов, что позволяет обрабатывать больше данных. Обеспечивает более тщательный анализ однородности данных, выявляя мелкие детали структуры. Перекрытие может выявить скрытую закономерность в данных.

Универсальный статистический тест Маурера (Maurer's Universal Statistical Test):

Оценивает, насколько хорошо последовательность «предсказывает» саму себя, используя теорию информации. Цель – проверить, зависит ли текущая информация от предыдущей, что может указать на скрытые данные. Ожидается случайность между элементами.

Тест на линейную сложность (The linear complexity test):

Оценивает, насколько сложно предсказать следующие биты последовательности на основе предыдущих. Если сложность низкая, это может означать, что данные управляются и могут содержать скрытые данные.

Тест на периодичность (The serial Test):

Оценивает наличие периодических элементов в последовательности. Периодичность может быть признаком зашумленности или попыток скрыть информацию.

Тест приблизительной энтропии (Approximate entropy test):

Оценивает, насколько сложно предсказать последовательности с повторениями. Высокая степень предсказуемости может указывать на наличие стеганографической информации.

Тест кумулятивных сумм (Cumulative Sums Test):

Оценивает кумулятивные суммы последовательности, определяя их колебания. Неправильные колебания могут сигнализировать о наличии структур в данных.

Тест на произвольные отклонения (Random excursion test):

Проводится анализ на отклонения в значениях последовательностей. Отклонения могут сигнализировать о наличии скрытой информации.

Другой тест на произвольные отклонения (Random excursion variant test):

Похожий на предыдущий с другой методологией. Анализирует различные статистические экскурсии и их корреляции. Подробный анализ на наличие закономерностей или аномалий в данных.

В работе предлагается использовать данный инструментарий для анализа битовых последовательностей слоев звуковых объектов, для оценки эффективности маскировки.

1.4. Характеристика атак на стегосистемы и описание модели нарушителя

Введение в уязвимости стегосистем

Стеганография, как метод сокрытия факта передачи информации, играет важную роль в системах защиты данных. Однако, несмотря на кажущуюся скрытность, стегосистемы уязвимы к различным видам атак. Основная задача нарушителя — выявить факт сокрытия данных, определить их местоположение и, по возможности, извлечь или повредить сообщение. Наиболее критичной считается атака на обнаружение, поскольку она нарушает сам принцип сокрытия — незаметность передачи.

Классификация атак на стегосистемы

Существуют следующие основные типы атак на стегосистемы:

1. Атака на обнаружение (стеганализ) — попытка определить наличие скрытого сообщения в предполагаемом контейнере (изображении, аудио [22,58,67-68,75,101], видео [59,77,90,100] и др.). Это наиболее распространенный тип атак, особенно в среде контроля цифрового трафика [109].

2. Атака на извлечение — направлена на получение скрытой информации без знания ключей или методов сокрытия.

3. Атака на уничтожение — цель которой заключается в повреждении или полном удалении скрытых данных путем внесения шумов или преобразований в контейнер.

4. Атака с известным контейнером — сравнение исходного и модифицированного контейнера для выявления различий и попытки восстановления сообщения.

5. Атака с известным сообщением — использование известного скрытого сообщения для анализа характеристик изменения контейнера и, впоследствии, построения модели атак.

Модель нарушителя

При моделировании угроз необходимо учитывать степень осведомленности и технические возможности потенциального нарушителя. Выделяют три основные модели:

- Частичный нарушитель — не обладает знаниями о конкретной стегосистеме, действует вслепую, используя обобщенные методы стеганализа.
- Информированный нарушитель — владеет информацией о применяемой стеганографической методике, но не имеет доступа к ключам или исходным контейнерам.
- Нарушитель с полным доступом — знает алгоритмы, ключи и может сравнивать оригинальный и стегоконтейнер, что делает его максимально опасным.

Каждая из моделей требует соответствующих мер защиты: от повышения стойкости алгоритма до использования адаптивных или переменных методов сокрытия.

Атака на обнаружение: особенности и методы

Атака на обнаружение (стеганализ) представляет собой процесс выявления присутствия скрытого сообщения в передаваемом объекте. Основные подходы включают:

- Статистический анализ — выявление аномалий в распределении пикселей, коэффициентов преобразования и других признаков, отличающих измененный контейнер от естественного.
- Машинное обучение — обучение классификаторов на больших выборках чистых и стеганографически модифицированных данных для автоматического определения вероятности наличия скрытой информации.
- Гибридные методы — комбинируют статистику и ИИ-подходы, обеспечивая более высокую точность обнаружения.

На практике атаки на обнаружение способны эффективно выявлять простые и предсказуемые схемы сокрытия информации. В то же время использование адаптивных и переменных методов (например, внедрение в сложные текстуры изображения) может существенно снижать вероятность обнаружения.

Риски информационной безопасности

Атаки на стегосистемы несут прямую угрозу конфиденциальности передаваемых данных. Потеря скрытности влечет за собой следующие риски:

- Компрометация передаваемой информации, в том числе конфиденциальной или персональной;
- Нарушение анонимности общения, особенно в условиях политической или корпоративной цензуры;
- Возможность модификации или искажения скрытых данных с последующим использованием в вредоносных целях;
- Утрата доверия к каналам связи, использующим стеганографию.

В условиях роста вычислительных мощностей и доступности интеллектуальных методов анализа, стегосистемы должны проектироваться с учетом вероятности атак на обнаружение и с применением механизмов, устойчивых к анализу различного уровня. Как отмечается в [80], фундаментальные исследования атак на стегосистемы подчеркивают необходимость разработки контрмер, внедряемых на этапе формирования стегоконтейнера.

Выводы по первой главе. Цель и задачи исследования

В главе рассмотрены особенности форматов записи звука. Показано, что все форматы делятся на три основных вида: звук без сжатия, звук со сжатием без потерь и звук со сжатием с потерями. При этом для звука, в отличие от изображений, биты характеризуются одномерным представлением, в виде одного или нескольких каналов.

При обработке звука в реальном времени присутствует, определяемая форматом, допустимая задержка, так, что звук обрабатывается блочно, что позволяет применять быстрые алгоритмы обработки.

Проведенные эксперименты показали, что анализ распределений значений с помощью дивергенции Кульбака–Лейблера или коэффициента корреляции Пирсона является недостаточным, для определения зависимостей битовых слоев и изменений в битовых слоях звуковых объектов без сжатия или битовых потоков звуковых объектов со сжатием. Поэтому предлагается ввести алгоритм расширенного анализа на основе NIST тестов на псевдослучайность, однако не в виде тестов, а в виде анализа без фактического сравнения с заданным показателем псевдослучайности, о чем пойдет речь во второй главе данной работы.

Для повышения маскировки скрытых сообщений в звуке предлагается использовать двухкомпонентный контейнер с учетом блочной обработки информации, позволяющий реализовать ряд подходов к маскировке информации с учетом имеющейся информации о покрывающем объекте.

В связи с этим поставлены следующие задачи исследования:

1. Разработать алгоритм многоуровневого стеганографического встраивания информации в звуковой покрывающий объект;
2. Разработать методику визуальной оценки свойств стеганографических систем;
3. Разработать комплекс математических моделей двухкомпонентных стеганографических систем для многоуровневого встраивания сообщений, в покрывающий объект в реальном времени;

Разработать технические решения двухкомпонентных стеганографических систем в виде программных реализаций

2. Математические модели подсистем встраивания сообщения в покрывающий объект из стеганографической системы

Под математической моделью стеганографической системы защиты информации рассматривается математическое описание подсистемы встраивания сигнала сообщения в сигнал контейнера на передающей стороне и математическое описание подсистемы извлечения сигнала сообщения из сигнала заполненного контейнера на принимающей стороне. Учитывая, что звуковые покрывающие объекты без сжатия информации и со сжатием информации описываются по-разному, рассмотрим их независимо.

В главе ставится задача четкого математического описания процесса встраивания сообщения в покрывающий объект и процесса извлечения сообщения из стеганографической системы. Учитывая, что обработка в реальном времени подразумевает оконный режим обработки информации, математические модели подразумевают встраивание информации в окно выборки отсчетов звукового покрывающего объекта.

В работе рассматриваются двухкомпонентные стеганографические системы [9-11,26-29,31-34,44,49,102]. Встраивание сообщения осуществляется за счет формирования двух компонент $z1$ и $z2$ и их последующего встраивания в покрывающий объект.

2.1. Математическая модель стеганографической системы использующей встраивание двух компонент в пределах одного отсчета с использованием функции исключающего ИЛИ

Звуковой ПО без сжатия представляет собой последовательность отсчетов заданной амплитуды с определенной частотой дискретизации. Наиболее распространенный звуковой формат, описываемый таким образом – формат WAVE [39]. Указанное описание именуется импульсно кодовой модуляцией (ИКМ). Таким образом звуковой ПО можно представить в виде множества X

отсчетов x, где $x \in X$. При этом сам отсчет представляет собой значение в заданном диапазоне, которое может быть представлено в виде заданного количества разрядов двоичного числа: $x = a_{x0} \| .. \| a_{xN-1}$, где N – количество бит описывающих отсчет x. Примем, что a_{xN-1}– старший разряд двоичного числа, a_0 – младший разряд двоичного числа, то есть $x = a_{xN-1} \cdot 2^{N-1} + a_{xN-2} \cdot 2^{N-2} \ldots + a_{x1} \cdot 2^1 + a_{x0} \cdot 2^0$. Рассматривая звук требуется учитывать, что звуковой сигнал знакопеременный. На знак выделяется отдельный бит, который мы в математической модели учитывать не будем, так как при встраивании скрытой информации он будет сохраняться.

Представим двухкомпонентный контейнер [10-11,27-29,31,33-34,37,49,102] в виде двухбитных значений $z1$ и $z2$. В общем случае компоненты $z1$ и $z2$ являются функцией сообщения и маскирующего сигнала ξ, однако, тогда на один бит сообщения придется два бита двух компонент, что приведет к снижению полезной нагрузки стеганографической системы. В работах [10-11,27-29,31,33-34,37,49,102] предлагается в качестве первой компоненты $z1$ использовать биты старших слоев ПО, а вторую компоненту представить в виде функции бита сообщения и первой компоненты. Это приведет к фактической модификации только при встраивании второй компоненты, так как первая использует неизменяемые слои ПО. Таким образом, при формировании первой компоненты имеют место две функции:

$$\mathbf{z1} = f_1(X) \qquad (2.1)$$

$$\mathbf{z2} = f_2(\mathbf{u}, \mathbf{z1}) \qquad (2.2)$$

В работах [10-11,27-29,31,33-34,37,49,102] предлагается следующий алгоритм определения первой компоненты двухкомпонентного контейнера - она выбирается из старших бит покрывающего объекта $z1 = a_{xi}$, где $i \in 1 \ldots N-1$. Значения i выбора первой компоненты $z1$ определяются алгоритмом, заданным разработчиком стеганографической системы. Возможные варианты: значение i является константой; значения i представляет собой конечный набор значений,

являющийся ключом системы; значения *i* определяются генератором случайных (псевдослучайных) чисел, известным передающей и принимающей сторонам.

Далее определяется значение второй компоненты $z2 = f(u, z1)$. В работах [10-11,27-29,31,33-34,37,49,102] предлагается способ формирования второй компоненты с помощью функции исключающего ИЛИ, примененной к биту сообщения и биту первой компоненты: $z2 = u \oplus z1$. Данная функция имеет широкое распространение в криптографии, однако выбор в качестве функции определения второй компоненты продиктован равномерностью значений таблицы истинности – в зависимости от комбинации входных значений, на выходе возможны два нуля и две единицы, что обеспечивает наилучшие условия маскировки (при равномерном распределении значений младшего битного слоя).

Учитывая, что выражение (2.1) может представлять сложную функцию многих бит, выражение (2.2) также будет более сложным, нежели одна логическая функция. Поэтому, в рамках математической модели используем наиболее общий вариант.

Стегосистема *Y* имеет структуру покрывающего объекта *X.* Каждый отсчет $y \in Y$ состоит из такого же количества бит, как и отсчет покрывающего объекта $y = a_{y_0} \| .. \| a_{y_{N-1}}$. Формирование стегосистемы осуществляется следующим образом: старшие биты a_{y_i} , где $i \in 1 \ldots N-1$ стегосистемы повторяют значения бит покрывающего объекта, в то время как младший бит $a_{y_0} = z2$.

Таким образом, математическая модель подсистемы встраивания одного бита сообщения в один *n*-ный отсчет ПО (рисунок 2.1), представленного в виде ряда бит, соответствующих разрядам двоичного представления отсчета имеет следующий вид:

$$\begin{cases} z1_n = f_1\left(x_n \setminus a_{x_{n0}}\right), \\ z2_n = f(u_n, z1_n) \\ a_{y_{ni}} = a_{x_{ni}}, i \in 1 \ldots N-1 \\ a_{y_{n0}} = z2_n \end{cases} \qquad (2.3)$$

Первая строка математической модели показывает, что первая компонента $z1_n$ определяется из всего массива бит отсчета, за исключением младшего бита. Вторая строка определяет вторую компоненту $z2_n$, как функцию первой компоненты и маскируемого бита u_n. Третья строка определяет старшие биты стегоконтейнера, за исключением младшего бита, как эквивалент ПО, в то время как младший бит определяется четвертой строкой модели, как вторая компонента стегоконтейнера $z2_n$ (встраиваемая компонента).

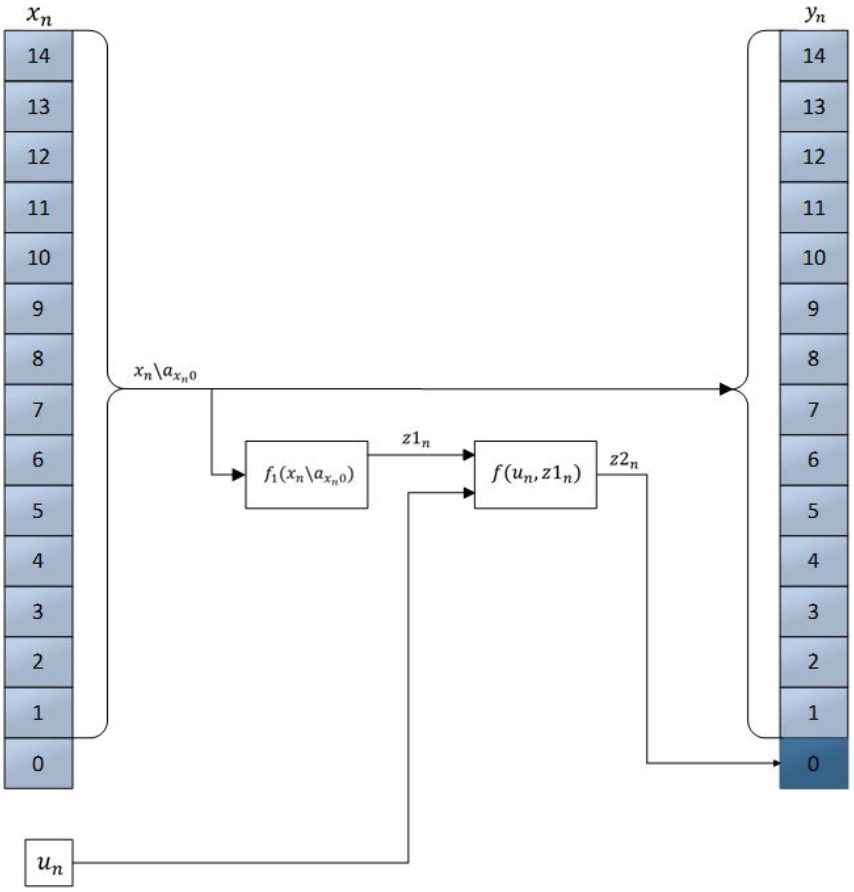


Рисунок 2.1 – Стеганографическая система, использующая встраивание одного бита сообщения в один n-ный отсчет ПО

В рамках данного исследования для генерации номера бита первой компоненты используется генератор псевдослучайных чисел, однако в общем случае используется ряд известных передающей и принимающей сторонам значений, который обозначим, как k_n (рисунок 2.2). Исходя из того, что для

определения второй компоненты используется функция сложения по модулю два, перепишем математическую модель в следующем виде:

$$\begin{cases} z1_n = a_{x_n k_n}, \\ z2_n = u_n \oplus z1_n \\ a_{y_n i} = a_{x_n i}, i \in 1 \ldots N-1 \\ a_{y_n 0} = z2_n \end{cases} \quad (2.4)$$

Полученная модель рассматривает встраивание одного бита сообщения в ПО. Однако, возможно и последовательное (многослойное) встраивание нескольких битов сообщения в пределах одного отсчета.

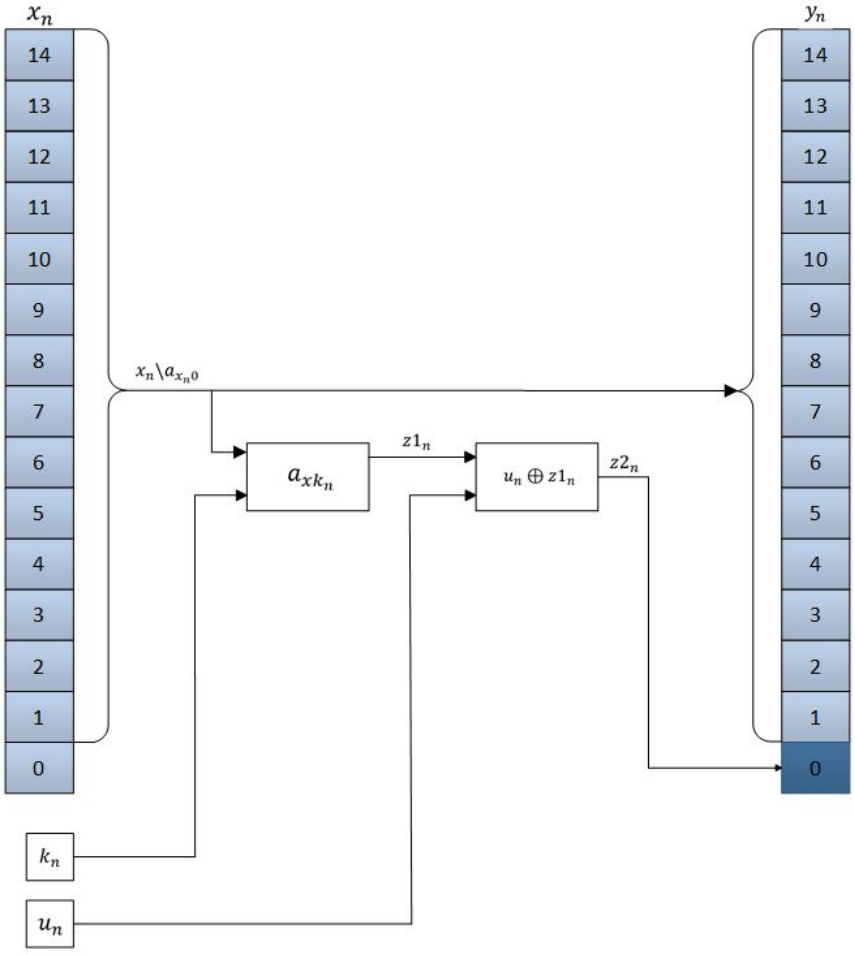


Рисунок 2.2 – Стеганографическая система, использующая встраивание одного бита сообщения в один *n*-ный отсчет ПО

Многослойное встраивание представляет собой итерационную процедуру, использующую несколько *L* встраиваний битов сообщения в разные битовые слои

ПО. Так как при встраивании скрытого сообщения в один из слоев он изменяется, последующее встраивание использует уже модифицированный ПО, как источник первой компоненты и объект для размещения второй. При этом следует учитывать, что при каждом встраивании происходит модификация ПО, при том, что для извлечения скрытой информации информация о первой и второй компонентах каждой итерации должна быть сохранена. В работе рассматривается встраивание от старшего слоя к младшему, однако данный подход не является единственным вариантом многослойного встраивания.

Встраивание начинается со старшего слоя. Тогда для каждой l итерации встраивания, $l \in 1 \ldots L$ номер слоя встраивания определится, как L-l. Обозначим каждый отсчет $x_{l,n}$, где l обозначает итерацию встраивания, а n номер отсчета. Для удобства понимания, в модели выходное значение каждой итерации обозначено как y_n. Однако, полное заполнение стегоконтейнера произойдет только при выполнении всех итераций (рисунок 2.3).

$$\begin{cases} z1_{l,n} = f_1\left(x_{l,n} \setminus a_{x_n\, 0..L-l}\right), \\ z2_{l,n} = f(u_{l,n}, z1_{l,n}) \\ a_{y_n\, i} = a_{x_n\, i},\ i \in L \ldots N-1 \\ a_{y_n\, L-l} = z2_{l,n} \end{cases} \qquad (2.5)$$

Первая строка модели указывает, что первая компонента текущей итерации l определяется слоями старше встраиваемого слоя L-l. Вторая строка определяет вторую компоненту, как функцию бита маскируемой информации и первой компоненты. Третья строка определяет старшие биты стегоконтейнера, начиная с уровня L и выше, как эквивалентные битам ПО. Остальные слои итерационно заполняются в соответствии с четвертой строкой модели компонентами $z2$.

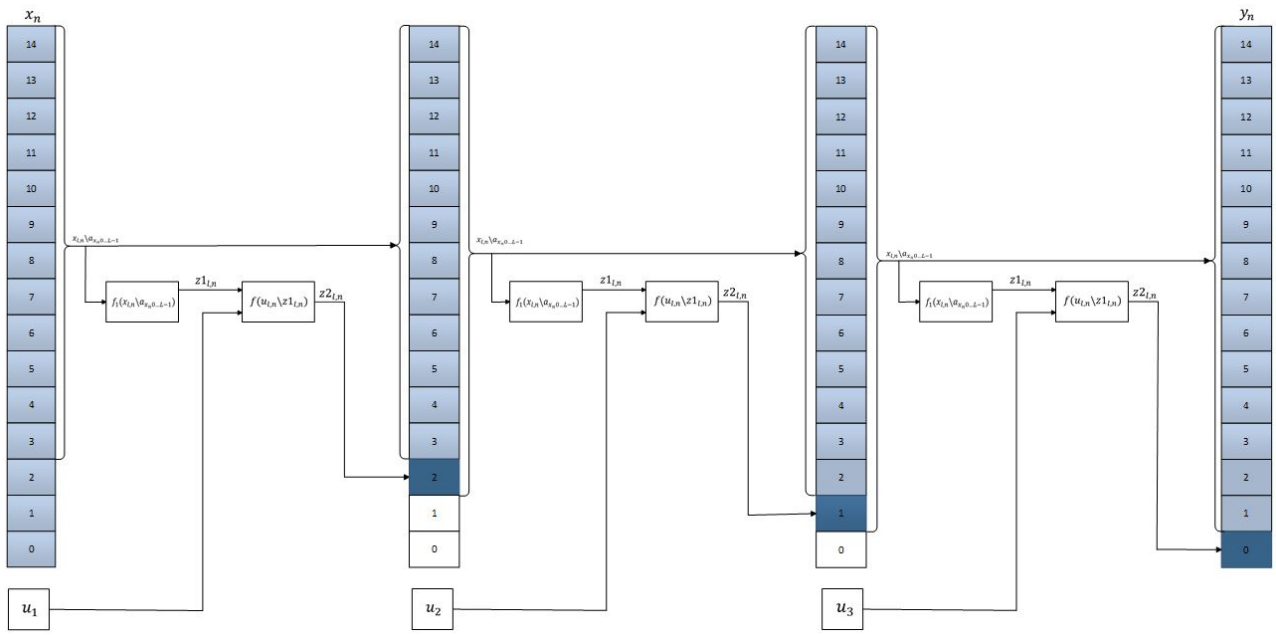


Рисунок 2.3 – Стеганографическая система, использующая последовательное (многослойное) встраивание нескольких битов сообщения в пределах одного отсчета

С учетом модели (2.4) многослойное встраивание (2.5) реализуется с помощью следующей модели, использующей для каждого встраиваемого бита ключ $k_{l,n}$ (рисунок 2.4):

$$\begin{cases} z1_{l,n} = a_{x\,k_{l,n}}, \\ z2_{l,n} = u_{l,n} \oplus z1_{l,n} \\ a_{y_n\,i} = a_{x_n\,i}, i \in L \ldots N-1 \\ a_{y_n\,L-l} = z2_{l,n} \end{cases} \qquad (2.6)$$

Полученные модели (2.3) и (2.5) являются математическими моделями встраивания двухкомпонентного контейнера в ПО, в то время как модели (2.4) и (2.6) являются частным случаем с имеющимся рядом координат бит первой компоненты и фиксированной функцией определения второй компоненты.

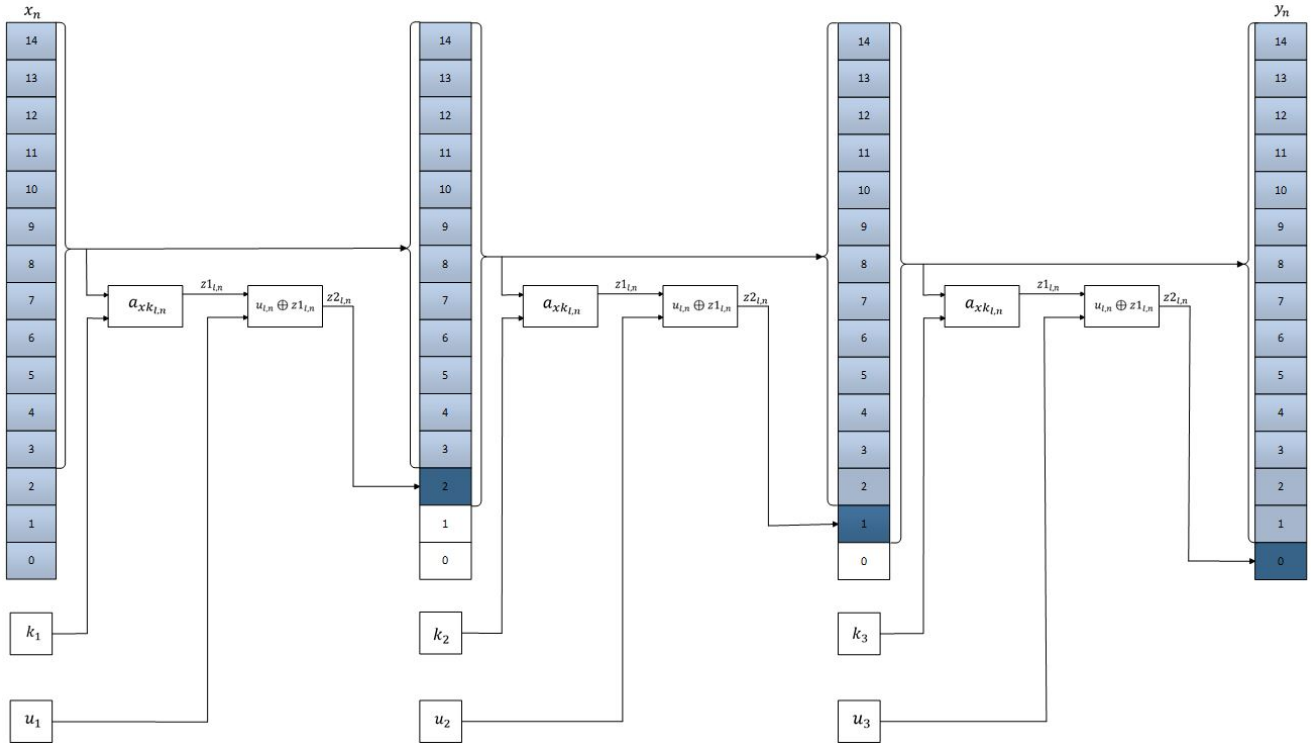


Рисунок 2.4 – Стеганографическая система, использующая последовательное (многослойное) встраивание бита и ключа $k_{l,n}$ сообщения в пределах одного отсчета

2.2. Математическая модель стеганографической системы использующей встраивание двух компонент в пределах окна фиксированного размера с использованием функции исключающего ИЛИ

В случае оконной обработки информации, возможности выбора первой компоненты расширяются за счет того, что доступно несколько отсчетов, а значит и первая компонента может выбираться не из текущего отсчета, а из ряда отсчетов. Основным отличием оконной обработки является усложненный выбор первой компоненты [43]. Так для каждого бита сообщения требуется определить первую компоненту не в пределах отсчета, где достаточно было только номера битового слоя, а в пределах массива. Иными словами, каждому u_n требуется поставить в соответствие ключ k_n, содержащий два значения – номер битового слоя и порядковый номер отсчета m в пределах обрабатываемого окна M, где

$m \in M$. Пусть $k_{n,0}$ – содержит номер битового слоя, определяющего слой из которого будет выбрана первая компонента стегоконтейнера, а $k_{n,1}$ – содержит номер отсчета, определяющий из какого отсчета обрабатываемого окна будет выбрана первая компонента стегоконтейнера. Для упрощения укажем в модели только ключ k_n, под которым будем понимать точное указание бита в пределах окна. Порядковый номер окна обозначим как w. Для упрощения модели допустим, что встраивается M отсчетов сообщения в окно размера M. Очевидно, что количество отсчетов сообщения может быть больше чем размер окна. В этом случае массив отсчетов сообщения разбивается на блоки размером M, после чего идет встраивание в пределах каждого окна ПО.

Таким образом, для каждого w окна модель встраивания будет иметь следующий вид:

$$\begin{cases} z1_{w,m} = f_1\left(x_{w,0..M-1} \setminus a_{xw,0..M-1\,0}\right), \\ z2_{w,m} = f(u_{w,m}, z1_{w,m}) \\ a_{y_{w,m\,i}} = a_{x_{w,m\,i}}, i \in 1 \ldots N-1 \\ a_{y_{w,m\,0}} = z2_{w,m} \end{cases} \qquad (2.7)$$

Первая строка полученной модели говорит о том, что первая компонента формируется из всего массива бит окна, за исключением младшего битового слоя. Вторая строка описывает формирование каждого последующего бита второй компоненты, как функции каждого последующего бита сообщения и каждого последующего бита первой компоненты. Третья строка модели показывает, что массив бит стегоконтейнера совпадает с массивом бит ПО за исключением младшего битового слоя, который формируется, в соответствии с четвертой строкой модели, последовательной записью бит второй компоненты [2].

Рассмотрим частный случай модели 2.7, которая, в соответствии с (2.4), перепишется следующим образом:

$$\begin{cases} z1_{w,m} = a_{x\,k_{w,m}}, \\ z2_{w,m} = u_{w,m} \oplus z1_{w,m} \\ a_{y_{w,m\,i}} = a_{x_{w,m\,i}}, i \in 1 \ldots N-1 \\ a_{y_{w,m\,0}} = z2_{w,m} \end{cases} \qquad (2.8)$$

Несмотря на сходство (2.8) и (2.3) их отличие значительно. Дело в том, что (2.8) применяется в пределах окна *w*, на что указывает адресация *m* вместо *n*, но самое главное отличие в том, что в модели (2.8) ключ $k_{w,m}$ представляет собой набор пар значений, описывающих битовый уровень и номер отсчета, определяющих позицию бита в массиве отсчетов окна *w*.

В случае многослойного встраивания в пределах окна математическая модель формируется на основе (2.5), с учетом оконной обработки (2.7) имеет вид:

$$\begin{cases} z1_{l,w,m} = f_1\left(x_{l,w,0..M-1} \setminus a_{x_{l,w,0..M-1}\,0..L-l}\right), \\ z2_{l,w,m} = f(u_{l,w,m}, z1_{l,w,m}) \\ a_{y_{w,m}\,i} = a_{x_{m}\,i}, i \in L \ldots N-1 \\ a_{y_{w,m}\,L-l} = z2_{l,w,m} \end{cases} \quad (2.9)$$

Полученная модель, в соответствии с (2.8) перепишется следующим образом:

$$\begin{cases} z1_{l,w,m} = a_{x\,k_{l,w,m}}, \\ z2_{l,w,m} = u_{l,w,m} \oplus z1_{l,w,m} \\ a_{y_{w,m}\,i} = a_{x_{m}\,i}, i \in L \ldots N-1 \\ a_{y_{w,m}\,L-l} = z2_{l,w,m} \end{cases} \quad (2.10)$$

2.3. Математическая модель стеганографической системы использующей встраивание двух компонент в пределах окна фиксированного размера с использованием условных функций определения второй компоненты стегоконтейнера

Полученные в предыдущих параграфах математические модели 2.3, 2.5, 2.7 и 2.9 не содержат в себе функцию формирования второй компоненты, которая определяется в моделях 2.4, 2.6, 2.8 и 2.10 на основе функции исключающее ИЛИ. Достоинством такого подхода является криптографическая стойкость данной функции, однако, есть и недостаток. В качестве недостатка следует отметить низкую адаптацию такой системы к статистическим перекосам в распределении значений битовых слоев. Например, если биты сообщения ***и*** имеют распределение

близкое к равномерному, то есть приблизительно равное количество нулей и единиц, то после применения функции исключающее ИЛИ, к массиву значений ***u*** и массиву ***z1***, который, к примеру, будет содержать одни нули, мы на выходе получим то же, примерно равное количество нулей и единиц. Для того, чтобы ввести элемент адаптации, предлагается использовать дополнительное условие, которое определит используемую функцию. Так, если в слоях ПО избыток нулей, то удобно использовать функцию И, так как она в таблице истинности имеет больше нулей или, в обратном случае, когда избыток единиц – удобно использовать функцию ИЛИ. Так как режим адаптации функции наиболее интересен при многослойном встраивании в оконном режиме, применим данный подход к модели 2.10 [3,46]. Введем параметр *c* который будет содержать сумму единичных бит из выборки заданного размера *C*. Выборка производится из заранее известных принимающей и передающей стороне бит старших слоев ПО. Если все биты выборки равны нулю, то используется логическая функция И. Если все биты равны единице, то используется логическая функция ИЛИ. В остальных случаях используется функция исключающее ИЛИ. Получим следующую математическую модель:

$$\begin{cases} z1_{l,w,m} = a_{xk_{l,w,m}}, \\ z2_{l,w,m} = u_{l,w,m} \wedge z1_{l,w,m} \quad при\ c = 0 \\ z2_{l,w,m} = u_{l,w,m} \vee z1_{l,w,m} \quad при\ c = C \\ z2_{l,w,m} = u_{l,w,m} \oplus z1_{l,w,m} \quad в\ остальных\ случаях \\ a_{y_{w,m}\,i} = a_{x_{m}\,i},\ i \in L \ldots N-1 \\ a_{y_{w,m}\,L-l} = z2_{l,w,m} \end{cases} \tag{2.11}$$

В полученной модели количество выборок в значительной степени определяет вероятность использования логических функций И и ИЛИ. Так, чем больше величина *C* тем менее вероятно сумма *c* будет равна нулю или единице. Таким образом, изменяя величину *C* в зависимости от слоя встраивания можно получить различную частоту применения логических функций И и ИЛИ и, как следствие, оказать влияние на степень маскировки информации (рис. 2.5).

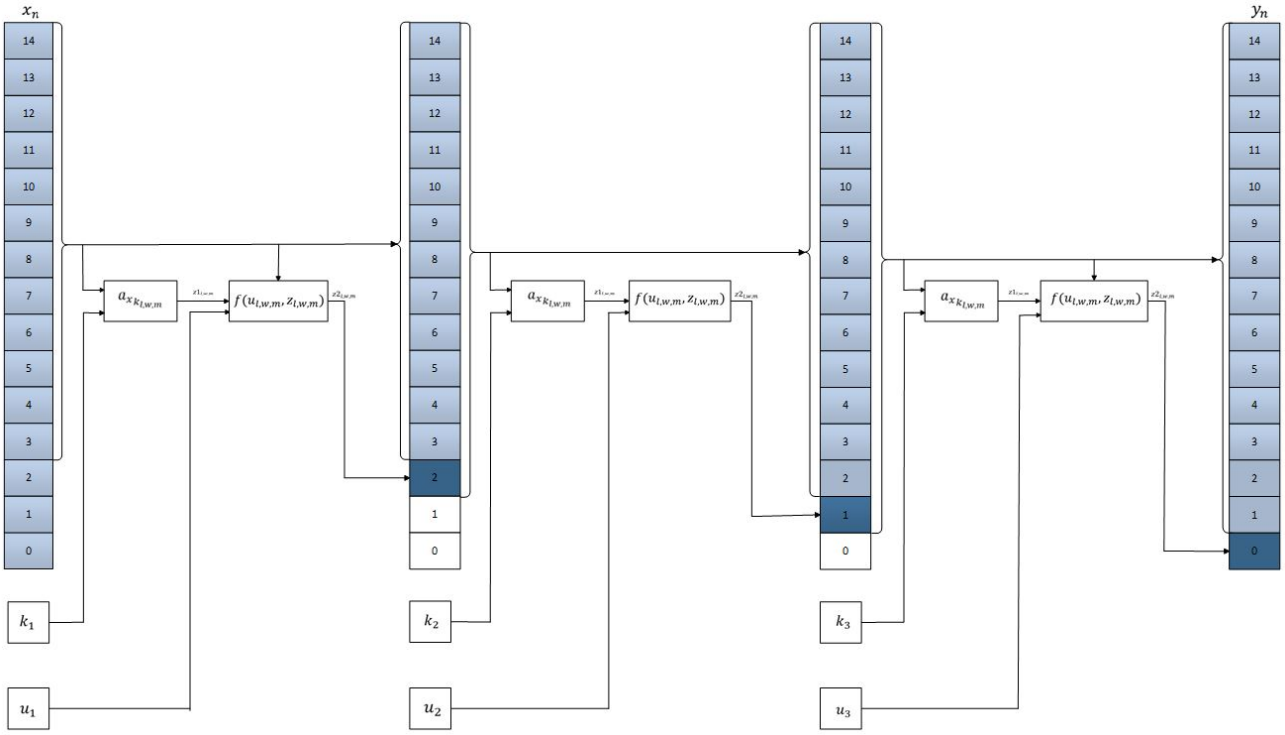


Рисунок 2.5 – Стеганографическая система, использующая встраивание двух компонент в пределах окна фиксированного размера с использованием условных функций определения второй компоненты стегоконтейнера

Следует отметить, что логические операции И и ИЛИ не обладают полной обратимостью, то есть при некоторых комбинациях входных значений выполнение обратной операции становится невозможным. Ниже приведены варианты входных данных, при которых процедура извлечения скрытого сообщения может быть корректно реализована.

Для функции И:

Встроенный бит (*z2*)	Бит ключа (*z1*)	Результат извлечения	Возможные биты сообщения	Заключение о возможности извлечения
0	0	0	0 или 1	Невозможно
0	1	0	0	Возможно
1	1	1	1	Возможно

Для функции ИЛИ:

Встроенный бит (*z2*)	Бит ключа (*z1*)	Результат извлечения	Возможные биты сообщения	Заключение о возможности извлечения
0	0	0	0	Возможно
1	0	1	1	Возможно
1	1	1	0 или 1	Невозможно

Когда на вход поступают значения бит, приводящие к неоднозначности при извлечении, соответствующий бит сообщения встраивается повторно — с использованием следующего по порядку значения ключа, обновленной первой компоненты *z1* нового значения параметра *c*. Принимающая сторона анализирует полученные значения стегосистемы, определяет примененную логическую функцию и, обнаружив неоднозначность при декодировании, пропускает данный бит, не включая его в результирующую последовательность.

Для иллюстрации данного процесса рассмотрим пример. Определим небольшой фрагмент данных покрывающего объекта, состоящий из шести отсчетов по восемь бит каждый. Пусть значения отсчетов равны:

$x_1=122_{10}=0111\ 1010_2$

$x_2=37_{10}=0010\ 0101_2$

$x_3=201_{10}=1100\ 1001_2$

$x_4=176_{10}=1011\ 0000_2$

$x_5=29_{10}=0001\ 1101_2$

$x_6=48_{10}=0011\ 0000_2$

Представим окно отсчетов покрывающего объекта в виде массива значений, показанного на рисунке 2.6. Процесс встраивания информации осуществляется в три младших разряда, обозначенные на рисунке 2.7.

		Номер отсчёта						
		1	2	3	4	5	6	
Номер разряда	7	0	0	1	1	0	0	Старший разряд
	6	1	0	1	0	0	0	
	5	1	1	0	1	0	1	
	4	1	0	0	1	1	1	
	3	1	0	1	0	1	0	
	2	0	1	0	0	1	0	
	1	1	0	0	0	0	0	
	0	0	1	1	0	1	0	Младший разряд

Рисунок 2.6 – Массив значений отсчетов покрывающего объекта

		Номер отсчёта						
		1	2	3	4	5	6	
Номер разряда	7	0	0	1	1	0	0	Старший разряд
	6	1	0	1	0	0	0	
	5	1	1	0	1	0	1	
	4	1	0	0	1	1	1	
	3	1	0	1	0	1	0	
	2	0	1	0	0	1	0	
	1	1	0	0	0	0	0	
	0	0	1	1	0	1	0	Младший разряд

Рисунок 2.7 – Процесс встраивания информации в три младших разряда

Для начала определим последовательность битов сообщения: *и*=0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0. Также зададим последовательность значений ключа, где первое значение указывает номер разряда, второе — номер отсчета. Поскольку ключ может использовать диапазон старших разрядов, установим следующие пределы:

– для встраивания во второй разряд диапазон старших разрядов составляет от 3 до 7,

– для встраивания в первый разряд — от 2 до 7,

– для встраивания в нулевой (младший) разряд — от 1 до 7.

Для упрощения примера будем считать, что ключ содержит относительные координаты: номера отсчетов имеют абсолютное значение (соответствуют фактическим номерам), а номера разрядов указываются относительно — как количество разрядов, расположенных выше того, в который производится встраивание. Например, если указан номер «1», а встраивание выполняется во второй разряд, то выбор осуществляется из третьего разряда.

Таким образом, последовательность ключа имеет вид: k = {3,4}, {3,2}, {2,2}, {2,1}, {2,4}, {3,6}, {1,3}, {1,1}, {2,4}, {2,4}, {3,1}, {3,3}, {2,1}, {1,3}, {1,5}, {2,6}, {3,4}, {2,2}. Помимо ключа, задается также параметр *cp*, содержащий координаты точек выборки. Его структура аналогична ключу, однако он формируется иначе: сначала задается количество точек выборки C, а затем для каждого встраиваемого бита определяются их координаты. Чтобы не усложнять пример, рассмотрим два набора координат при C=3, то есть для каждого бита определяются три точки выборки:

cp={1,2}, {3,5}, {2,6}; {1,5}, {2,1}, {4,2}; …

После определения всех исходных данных рассмотрим процесс встраивания.

Встраивание первого бита сообщения.

Схема процесса представлена на рисунке 2.8. Встраивание выполняется во второй разряд первого отсчета. Значение первого бита сообщения u_1=0. Согласно ключу k_1={3,4}, значение соответствующего бита первой компоненты $z1$=1.

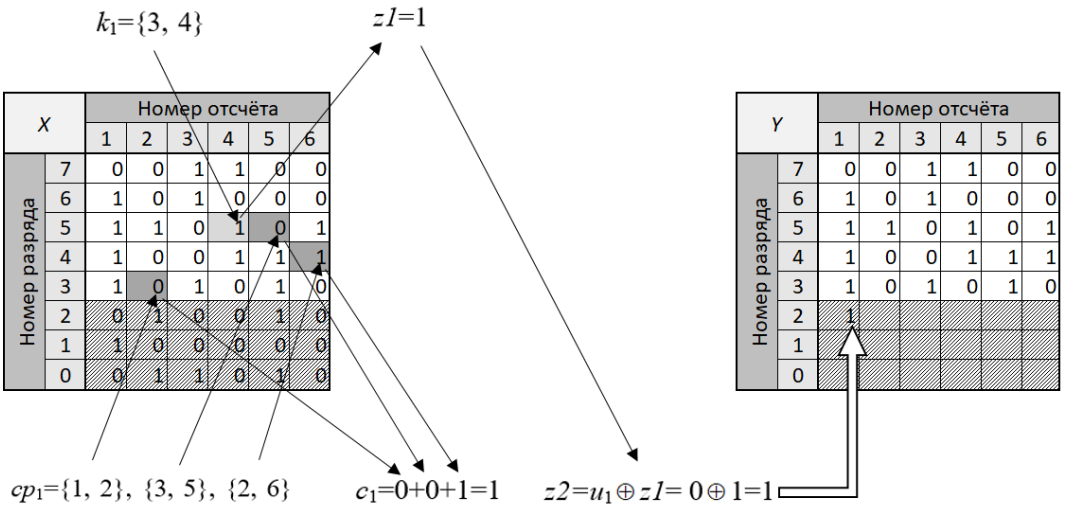


Рисунок 2.8 – Процесс встраивания первого бита сообщения

Для вычисления суммы c используем координаты cp_1={1,2}, {3,5}, {2,6}. Определив значения разрядов в указанных позициях, получаем: c_1=0+0+1=1. Следовательно, используется логическая операция исключающее ИЛИ (XOR). Тогда: $z2= u_1 \oplus z1= 0 \oplus 1=1$. Таким образом, во второй разряд первого отсчета встраивается значение 1.

Встраивание второго бита сообщения.

Схема процесса показана на рисунке 2.9. Встраивание выполняется во второй разряд второго отсчета. Значение бита сообщения u_2=1. Согласно ключу k_2={3,2}, значение первой компоненты $z1$=1. Для вычисления суммы с используем координаты cp_2={1,5}, {2,1}, {4,2}, что дает: c_1=1+1+0=2. Применяется та же логическая операция исключающее ИЛИ, и тогда: $z2=u_2 \oplus z1=1 \oplus 1=0$.

Следовательно, во второй разряд второго отсчета встраивается значение 0.

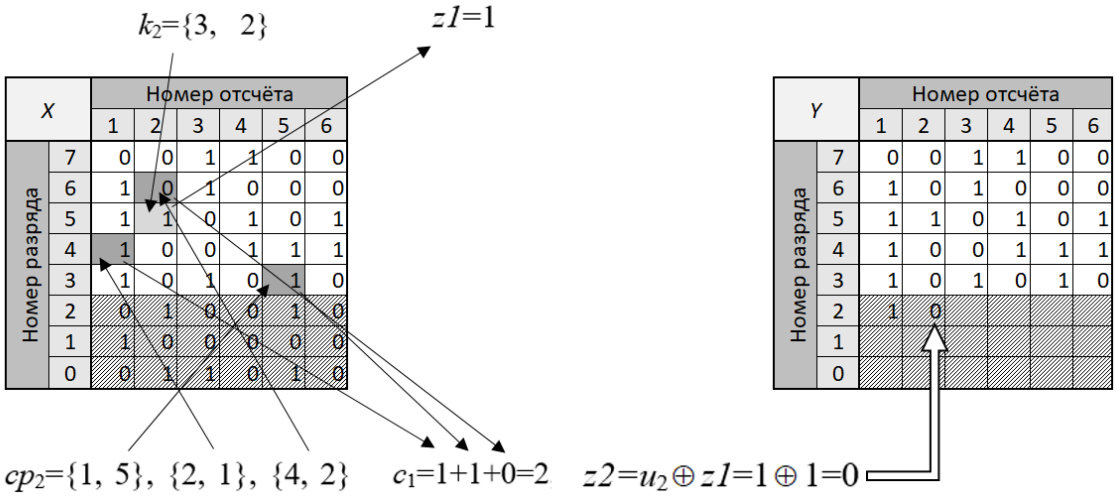


Рисунок 2.9 – Процесс встраивания второго бита сообщения

Для дальнейшего анализа сведем входные данные и результаты вычислений в таблицу (табл. 2.1). Значения параметров cp и сумм c подобраны таким образом, чтобы наглядно продемонстрировать особенности функционирования алгоритма [28]. Первые два примера в таблице соответствуют описанным выше случаям.

Можно отметить, что в ситуациях, когда логические функции И или ИЛИ не позволяют корректно извлечь встроенную информацию, встраивание второй компоненты все же выполняется. При этом бит сообщения повторно внедряется до тех пор, пока не будет обеспечена возможность его корректного извлечения.

На принимающей стороне, если при декодировании возникает неопределенность, соответствующий бит просто пропускается. Результирующее состояние массива после встраивания показано на рисунке 2.10.

Таблица 2.1 – Данные для встраивания сообщения в покрывающий объект

№ бита сообщ.	*u*	*k*	*z1*	*c*	*C*	функция	*z2*	примечание
1	0	{3, 4}	1	1	3	⊕	1	Корректное извлечение
2	1	{3, 2}	1	2	3	⊕	0	Корректное извлечение
3	0	{2, 2}	0	2	3	⊕	0	Корректное извлечение
4	0	{2, 1}	1	1	3	⊕	1	Корректное извлечение
5	1	{2, 4}	1	1	3	⊕	0	Корректное извлечение
6	0	{3, 6}	1	2	3	⊕	1	Корректное извлечение
Встраивание в старший разряд диапазона завершено. Переход на слой ниже.								
7	1	{1, 3}	1	0	3	∧	1	Корректное извлечение
8	1	{1, 1}	1	3	3	∨	1	Повторное встраивание
8	1	{2, 4}	1	2	3	⊕	0	Корректное извлечение
9	1	{2, 4}	1	0	3	∧	1	Корректное извлечение
10	0	{3, 1}	1	3	3	∨	1	Повторное встраивание
10	0	{3, 3}	0	3	3	∨	0	Корректное извлечение
Встраивание в следующий младший разряд диапазона завершено. Переход на слой ниже.								
11	1	{2, 1}	1	1	3	⊕	0	Корректное извлечение
12	0	{1, 3}	1	2	3	⊕	1	Корректное извлечение
13	0	{1, 5}	1	0	3	∧	0	Корректное извлечение
14	1	{2, 6}	1	3	3	∨	1	Повторное встраивание
14	1	{3, 4}	1	2	3	⊕	0	Корректное извлечение
15	0	{2, 2}	0	3	3	∨	0	Корректное извлечение
Встраивание в самый младший разряд завершено								

X		Номер отсчёта					
		1	2	3	4	5	6
Номер разряда	7	0	0	1	1	0	0
	6	1	0	1	0	0	0
	5	1	1	0	1	0	1
	4	1	0	0	1	1	1
	3	1	0	1	0	1	0
	2	0	1	0	0	1	0
	1	1	0	0	0	0	0
	0	0	1	1	0	1	0

Y		Номер отсчёта					
		1	2	3	4	5	6
Номер разряда	7	0	0	1	1	0	0
	6	1	0	1	0	0	0
	5	1	1	0	1	0	1
	4	1	0	0	1	1	1
	3	1	0	1	0	1	0
	2	1	0	0	1	0	1
	1	1	1	0	1	1	0
	0	0	1	0	1	0	0

Рисунок 2.10 – Массив данных результата после встраивания сообщения

Выводы по второй главе

Во второй главе получены математические модели для двухкомпонентных стеганографических систем, использующих в качестве первой компоненты биты старших слоев покрывающего объекта и логическую связь между битами встраиваемого сообщения и первой компоненты для формирования встраиваемой в младший битовый слой второй компоненты.

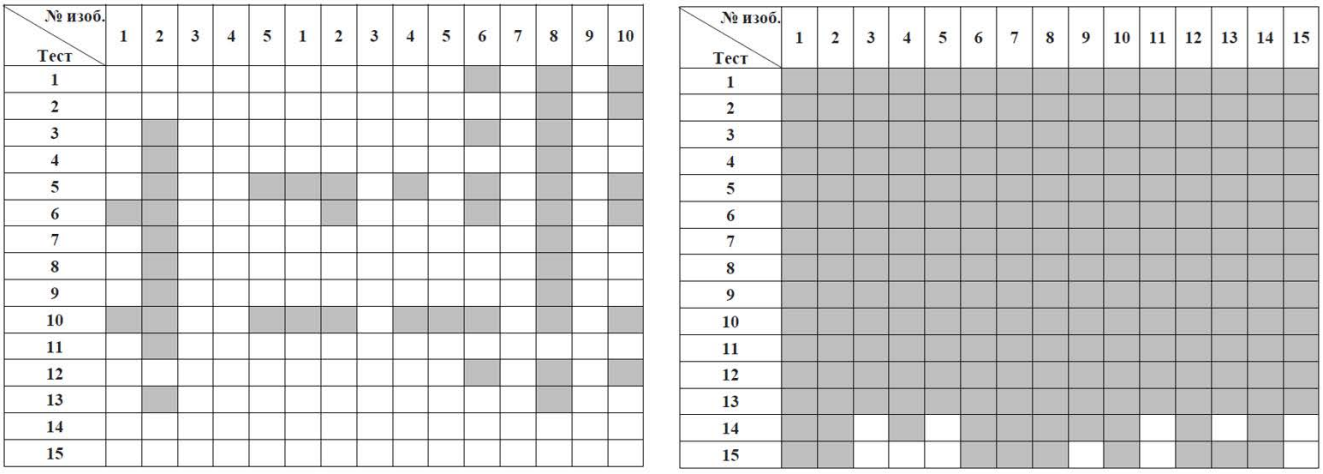
Получены модели, как для встраивания одного бита сообщения в пределах одного отсчета, ряда бит сообщения в пределах окна фиксированного размера, а также модели для многослойного встраивания битов сообщения.

Для многослойного встраивания битов сообщения, применяемого к окну обрабатываемых данных, получено решение, использующее различные логические функции, а именно И, ИЛИ и исключающее ИЛИ в зависимости от состава бит старших слоев ПО. Данное решение позволяет адаптировать систему к статистическим изменениям между битовыми слоями ПО и снизить заметность модификации ПО при многослойном встраивании двухкомпонентной стегосистемы.

3. Методика анализа битовых последовательностей на основе NIST тестов

Исследование статистических свойств покрывающих объектов с целью формирования статистического «портрета» битовой последовательности представляет собой важную задачу, так как позволяет оценить эффективность стеганографического алгоритма.

Самым распространенным подходом для анализа статистических параметров является анализ распределений битовых значений. Однако, практика показала, что анализ распределений не дает достаточной информации о битовой последовательности. С этой целью в работе [24] использован подход применением NIST тестов для анализа на псевдослучайность. В работе предлагалось провести тесты и, сравнивая результаты тестов для покрывающего объекта и стегосистемы определить расхождения. На рисунке 3.1 приведен пример использования такого подхода [24].



а. б.

Рисунок 3.1 – Пример использования NIST тестов для анализа полутоновых изображений; а – без вложений, б – с полным вложением в наименьший значащий бит зашифрованного сообщения.

Видно, что подход использующий NIST тесты позволяет выявить дополнительные статистические параметры. Однако, здесь использовано

применение тестов на псевдослучайность. Мы видим только результат проверки – является последовательность случайной или нет. Рассмотрим, как можно улучшить данный подход.

3.1. Анализ битовых последовательностей на основе NIST тестов

Всего в стандарте [53] описаны 15 тестов, сведенные в таблицу 3.1.

Таблица 3.1 – Названия тестов, входящих в стандарт NIST и количество результатов тестов в соответствии с выбранными параметрами тестирования

Номер теста	Название теста		Количество результатов
1	Frequency (monobit) test	Частотный побитовый тест	1
2	Frequency Test within a Block	Частотный блочный тест	1
3	Runs Test	Тест на последовательность одинаковых битов	1
4	Test for the Longest Run of Ones in a Block	Тест на самую длинную последовательность единиц в блоке	1
5	Binary Matrix Rank Test	Тест рангов бинарных матриц	1
6	Discrete Fourier Transform (Spectral) Test	Спектральный тест	1
7	Non-overlapping Template Matching Test (8 бит)	Тест на совпадение неперекрывающихся шаблонов	74
8	Overlapping Template Matching Test	Тест на совпадение перекрывающихся шаблонов	1
9	Maurer’s «Universal Statistical» Test	Универсальный статистический тест Маурера	1
10	Linear Complexity Test	Тест на линейную сложность	1
11	Serial Test	Тест на периодичность	2
12	Approximate Entropy Test	Тест приблизительной энтропии	1
13	Cumulative Sums (Cusum) Test	Тест кумулятивных сумм	2
14	Random Excursions Test	Тест на произвольные отклонения	8
15	Random Excursions Variant Test	Другой тест на произвольные отклонения	18

Интересной особенностью тестов является то, что некоторые из них могут иметь различное количество результатов. Так, например, седьмой тест «Тест на совпадение неперекрывающихся шаблонов» анализирует появление шаблонов в битовой последовательности. Количество шаблонов, определяемое их размером, определяет количество выходных данных. В работе предлагается использовать 8 битные шаблоны, что, в соответствии с требованиями тестов формирует блок из

74 выходных результатов. Общее количество результатов можно увидеть в правом столбце таблицы 3.1

В стандарте все тесты сведены к получению параметра *p*, в соответствии с нулевой гипотезой [24,53] если *p* больше, чем 0.01, то тестируемая последовательность является случайной. Однако, в задаче анализа не столь важен факт случайности битовых последовательностей, сколько важен факт установки статистических взаимосвязей между битовыми последовательностями. Поэтому предлагается опустить факт тестирования по показателю 0.01 и остановиться на сборе и анализе значений параметров *p*. Так как величина *p* принимает значения от 0 до 1, в результате проведения тестов мы получаем 114 (в соответствии с таблицей 3.1) отсчетов от 0 до 1. Взаимную связь между проведенными исследованиями, для отсчетов *p*, можно проводить с помощью коэффициента корреляции или других средств сравнения. Рассмотрим пример использования данного подхода.

Смоделируем NIST тесты в соответствии с описанием [53]. На рисунке 3.2 приведена функция, формирующая массив значений параметров *p*. Так как предлагаемая методика имеет отличие от NIST тестов, а именно исключает завершающий этап сравнения, далее будем обращаться к данной процедуре как к «тестам».

Заметим, что порядок следования отсчетов в сформированном массиве имеет привязку к последовательности оригинальных NIST тестов, но сами отсчеты не связаны друг с другом, а их расположение вдоль оси абсцисс является условным.

```
def NIST_test(data):
    Result_rng=np.zeros([114],dtype=float)
    Result_rng[0]=Test1(data)
    Result_rng[1]=Test2(data)
    Result_rng[2]=Test3(data)
    Result_rng[3]=Test4(data)
    Result_rng[4]=Test5(data)
    Result_rng[5]=Test6(data)
    Result_rng[6:80]=Test7(data)
    Result_rng[80]=Test8(data)
    Result_rng[81]=Test9(data)
    Result_rng[82]=Test10(data)
    Result_rng[83:85]=Test11(data)
    Result_rng[85]=Test12(data)
    Result_rng[86:88]=Test13(data)
    Result_rng[88:96]=Test14(data)
    Result_rng[96:114]=Test15(data)
    return Result_rng
```

Рисунок 3.2 – Функция формирования результатов тестов

Проведем тестирование встроенного в Python генератора случайных чисел и сравним результат с младшим битовым слоем аудио-потока. В качестве тестового аудиофайла выбран файл в формате WAVE, представленный в импульсно-кодовой модуляции (ИКМ).

Временные зависимости для двух каналов представлены на рисунке 3.3.

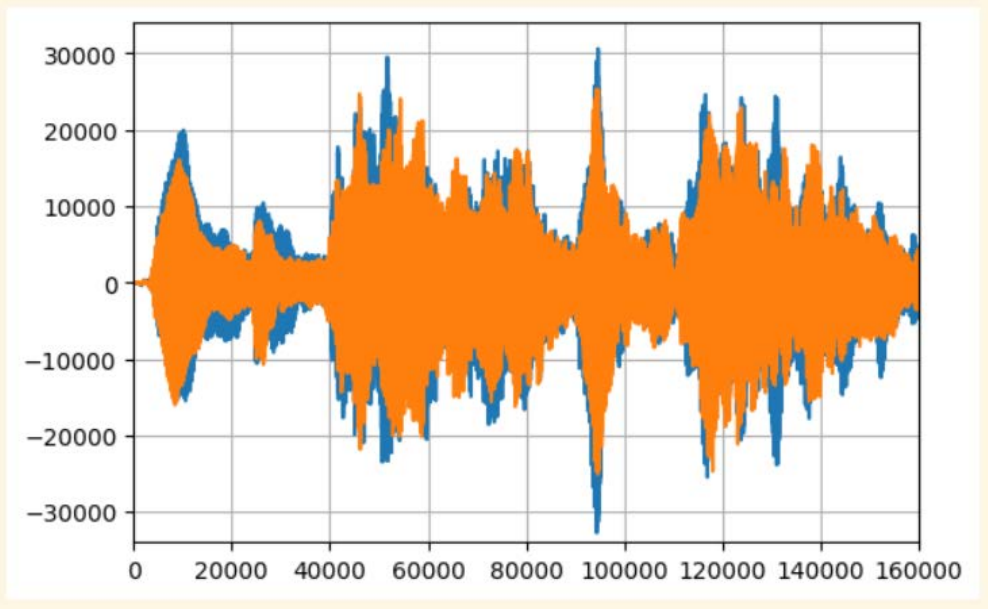


Рисунок 3.3 – Временные зависимости звукового сигнала: синий левый канал, оранжевый – правый

Параметры сигнала: 2 канала, частота дискретизации 44100 Гц, 16 бит на отсчет. Для проведения тестирования данных аудиофайла произведено разбитие на битовые слои. При этом знак выделен из битовой последовательности в отдельный ряд, и анализ проводился только по модулю значений. Определим распределение значений ГПСЧ. На рисунке 3.4 показана гистограмма распределения значений ГПСЧ, для количества точек n=160965. Количество точек определено длиной аудиофайла.

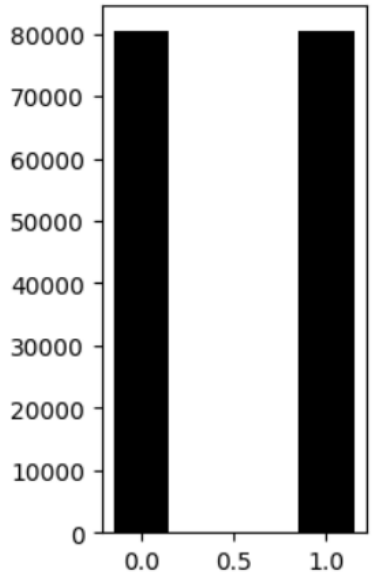


Рисунок 3.4 – Распределение значений ГПСЧ Python

Для сравнения, распределения значений для трех младших слоев аудиофайла приведены на рисунке 3.5. Видно, что распределение значений в слоях практически не отличается. Таким образом, провести какое-либо сравнение между сгенерированными ГПСЧ отсчетами и отсчетами младших битовых слоев аудиофайла на основе распределения значений бит невозможно. Попробуем проанализировать результаты 15 тестов на основе NIST.

На рисунке 3.6 приведен результат тестирования ряда, сгенерированного встроенным генератором псевдослучайных чисел (ГПСЧ). Сравним с результатом вычислений для трех младших битовых слоев аудиофайла. На рисунке 3.7 приведен результат вычисления тестов для младшего битового слоя.

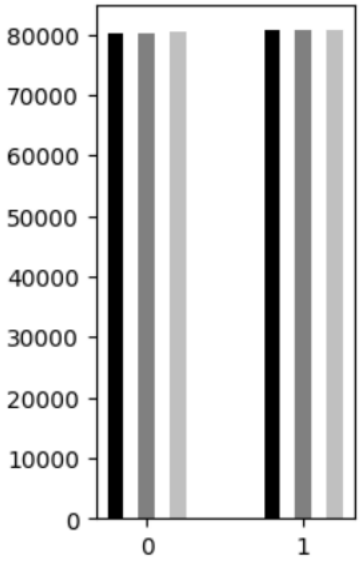


Рисунок 3.5 – Распределение значений для трех младших слоев аудиофайла: черный – 0 слой, темно-серый – 1 слой, светло-серый – 2 слой.

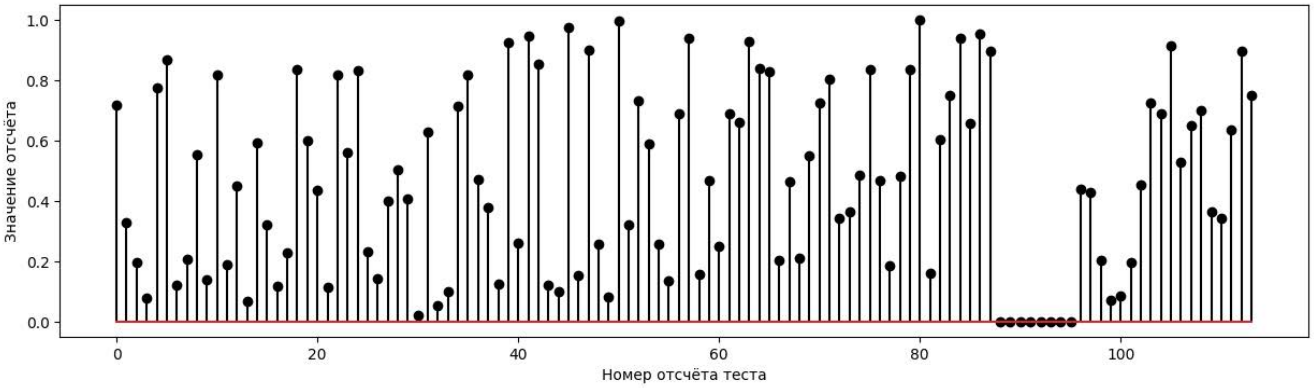


Рисунок 3.6 – Результат тестирования ряда псевдослучайных чисел

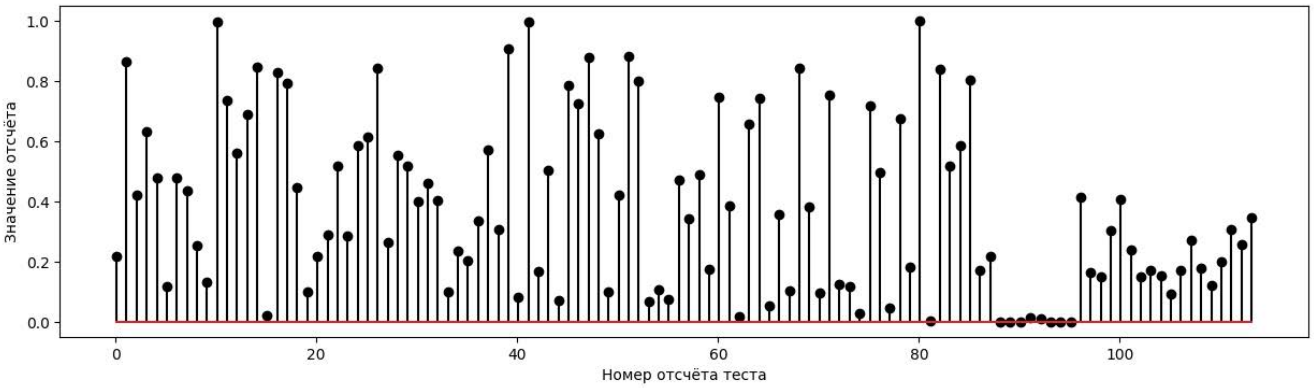


Рисунок 3.7 – Результат тестирования младшего битового слоя аудиофайла

На рисунках 3.8 и 3.9 приведены результаты тестов 1 и 2 битовых слоев аудиофайла соответственно.

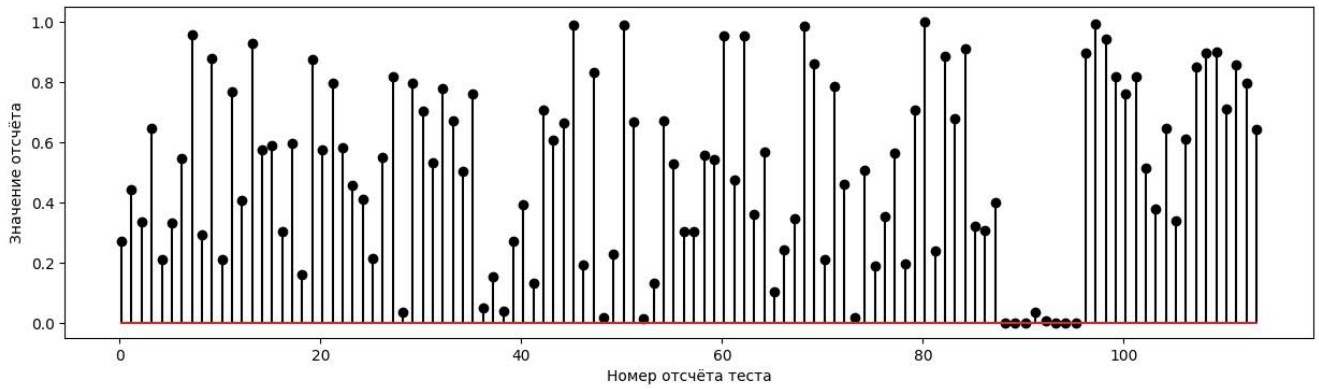


Рисунок 3.8 – Результат тестирования младшего битового слоя аудиофайла

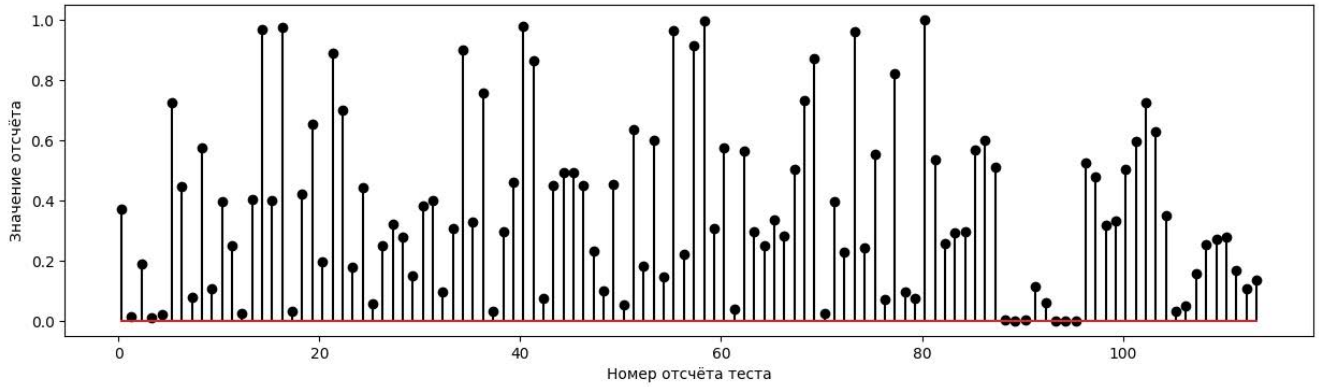


Рисунок 3.9 – Результат тестирования младшего битового слоя аудиофайла

Визуальный анализ не позволяет выявить строгие зависимости между полученными результатами. Тем не менее, они разные, в отличие от распределения значений, что позволяет сделать вывод о возможности извлечения информации из полученных результатов. Однако использование данной информации в задачах стеганографии представляет собой сложную задачу. С одной стороны, результаты тестов сложно формализовать, с другой их вычисление занимает достаточно длительное время. Так вычисление значений и построение каждого из приведенных выше результатов занимает более 10 минут (при средней мощности компьютера). При количестве отсчетов в анализируемой выборке свыше одного миллиона вычисление затягивается на часы. Целесообразно исключить тесты, чья вычислительная сложность слишком

высока, а информативность в задачах стеганографии минимальна. Проведем эмпирическую оценку времени вычислений для каждого из 15 тестов и исключим наиболее затратные по времени. В таблице 3.2 приведены тесты, время их вычисления и время вычисления одного отсчета массива результатов.

Таблица 3.2 – Время вычисления каждого из тестов

Номер теста	Название теста	Время вычисления, с.	Количество результатов	Время вычисления одного отсчета, с.
1	Frequency (monobit) test	0.142	1	0.142
2	Frequency Test within a Block	0.140	1	0.140
3	Runs Test	0.226	1	0.226
4	Test for the Longest Run of Ones in a Block	0.025	1	0.025
5	Binary Matrix Rank Test	0.820	1	0.820
6	Discrete Fourier Transform (Spectral) Test	0.322	1	0.322
7	Non-overlapping Template Matching Test (8 бит)	215.8	74	2.916
8	Overlapping Template Matching Test	2.8	1	2.8
9	Maurer’s “Universal Statistical” Test	0.716	1	0.716
10	Linear Complexity Test	30.1	1	30.1
11	Serial Test	41.4	2	20.7
12	Approximate Entropy Test	64.8	1	64.8
13	Cumulative Sums (Cusum) Test	0.785	2	0.363
14	Random Excursions Test	17.5	8	0.25
15	Random Excursions Variant Test	14.9	18	0.189

Оценку эффективности того или иного теста в задачах стеганографии можно провести только на основе модели встраиваемых данных.

3.2. Модель сообщения

Сообщение в общем случае является случайной последовательностью бит, однако, следует учитывать, что далеко не всегда его статистические свойства близки свойствам ГСЧ. Наиболее часто встречающиеся сообщения представляют собой текст или изображения. Пересылка звука возможна, но из-за значительного объема нецелесообразна. Во многих работах оценка стеганографических систем

строится на основе анализа распределений значений до и после встраивания скрытой информации с применением дивергенции Кульбака-Лейблера или коэффициента корреляции Пирсона. Тогда сообщение подбирается таким образом, чтобы отличаться от значений бит области встраивания статистически, в противном случае факт встраивания сложно зафиксировать даже при полном заполнении области встраивания.

Такой подход, с одной стороны, позволяет оценить степень вносимых при встраивании сообщения в покрывающий объект искажений, с другой стороны, не в полной мере соответствует реальности, где сообщение может подвергаться предварительному кодированию [23]. В работе предлагается расширить модель сообщения, чтобы она соответствовала различным задачам.

В стеганографических системах встраиваемое сообщение, как правило, подвергается предварительному криптографическому шифрованию. Существуют различные варианты шифров. Для выбора обратимся к актуальному протоколу передачи информации Transport Layer Security (TLS) версии 1.3 [105]. В соответствии с протоколом и, учитывая распространенность выберем шифр AES в режиме гаммирования (GCM – Galois Counter Mode). Как альтернативный вариант используем шифр Кузнечик (ГОСТ и RFC 9367 для TLS 1.3) так же в режиме гаммирования [7]. Структурная схема блочного шифрования в режиме GCM приведена на рисунке 3.10.

Таким образом, представим обобщенную модель сообщения в виде трех сигналов: незашифрованного, зашифрованного шифром AES и зашифрованного шифром Кузнечик. Так как нас интересует только статистические свойства зашифрованной информации, данные аутентификации можно опустить.

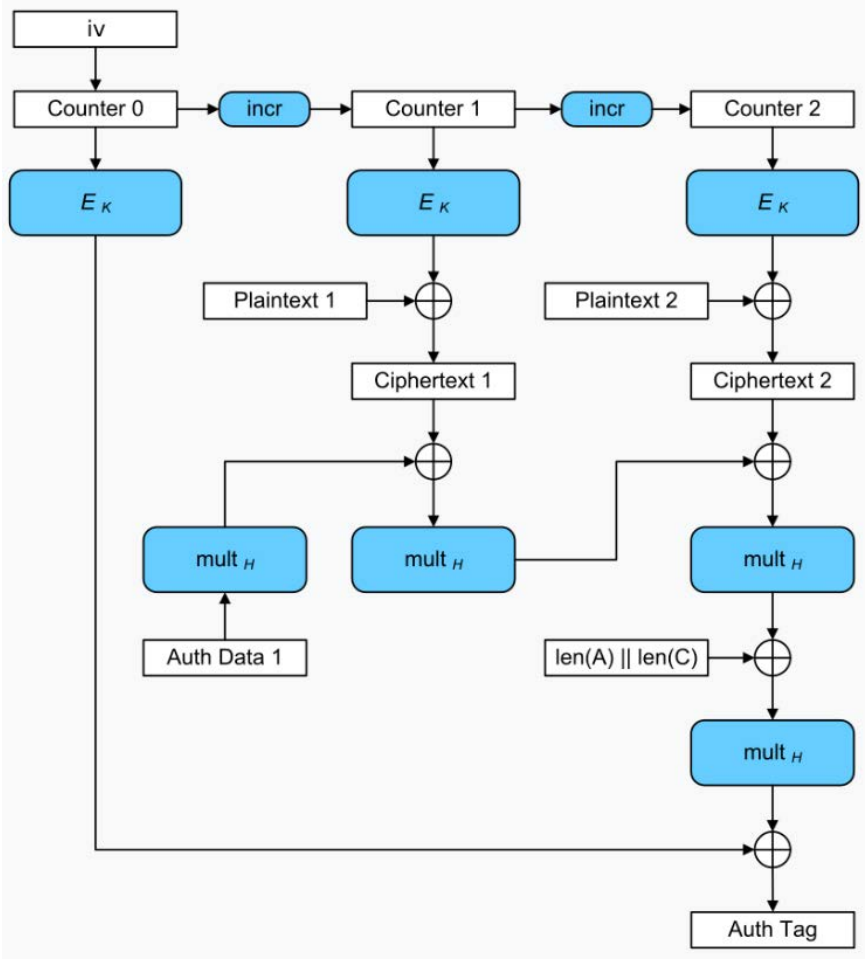


Рисунок 3.10 – Структурная схема шифрования в режиме счетчика Галуа

В качестве передаваемых данных в данной работе выбран pdf файл [24], приблизительным размером 5 Мб, содержащий текст, формулы и рисунки. Построим модель статистического анализа данных файла. Так как информация в файле записана в байтах, расположим байты в виде бит друг за другом.

Проведем анализ данных, ограничив размер ряда 160 000 значений (20 000 байт). На рисунке 3.11 приведен результат вычислений всех тестов для выбранного окна. Видно, что большое количество тестов дают малые значения, что говорит о большом количестве зависимостей внутри данных.

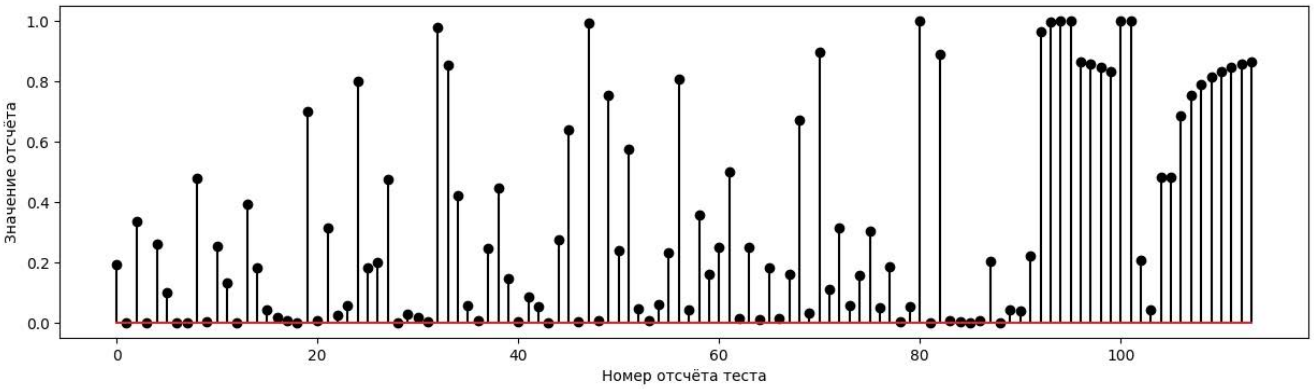


Рисунок 3.11 – Тест данных файла monography.pdf

Проведем моделирование шифрования данных с помощью шифра AES-256 [41]. Программа, реализующая шифрование в режиме счетчика Галуа приведена на рисунке 3.12. В модели использованы вспомогательные функции: dtb() – преобразование скалярного значения в массив бит, с указанием их количества; bits_to_block() – функция, преобразующая ряд бит в квадратный массив из 16 байт, размером 4 на 4.

```
#Определение AES-GCM
def AES_256_GCM(data,key_256):
    b_num=np.int64(np.floor(len(data)/128))
    e_data=np.zeros([b_num*128],dtype=int)
    w=KeyExpansion256(key_256)
    for i in range(b_num):
        Counter=bits_to_block(dtb(i,128))
        e_data[128*i:128*i+128]=block_to_bits(np.reshape(AES256(Counter,w),(16),order="F")
                                              ^bits_to_block(data[128*i:128*i+128]))
    return e_data
```

Рисунок 3.12 – Реализация шифра AES в режиме GCM

Проведем шифрование блока данных. На рисунке 2.13 приведен результат тестирования зашифрованного фрагмента размером 20 000 байт.

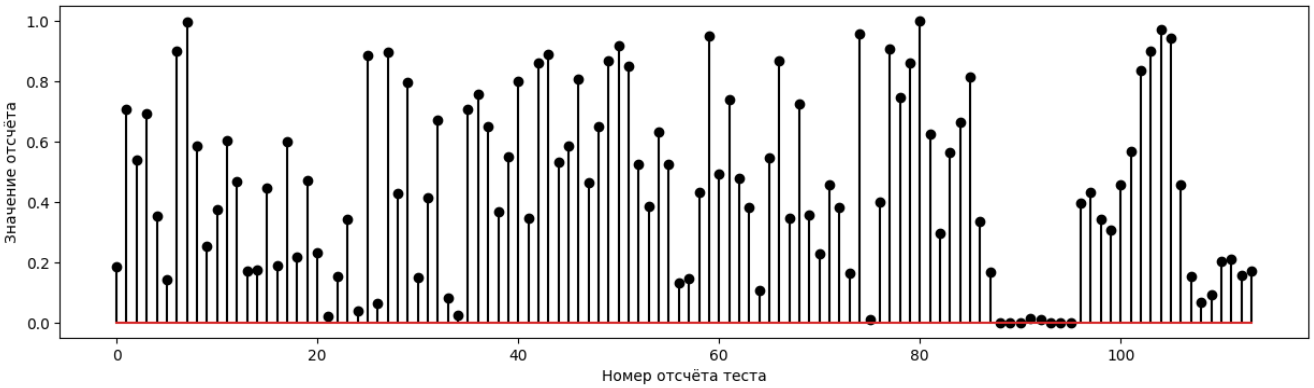


Рисунок 3.13 – Тест данных, зашифрованных AES в режиме GCM

Видно, что количество «пройденных» тестов увеличилось. Аналогично, рассмотрим шифрование с помощью шифра Кузнечик [42]. На рисунке 3.14 приведен код программы, реализующей шифрование Кузнечик в режиме счетчика Галуа.

```
#Определение Кузнечик-GCM
def Kuznechik_GCM(data,key_256):
    b_num=np.int64(np.floor(len(data)/128))
    e_data=np.zeros([b_num*128],dtype=int)
    key=KeySchedule(key_256)
    for i in range(b_num):
        Counter=bits_to_block(dtb(i,128))
        e_data[128*i:128*i+128]=block_to_bits(Kuznechik(Counter,key)^
                                              bits_to_block(data[128*i:128*i+128]))
    return e_data
```

Рисунок 3.14 – Реализация шифра Кузнечик в режиме GCM

На рисунке 3.15 приведен результат тестирования зашифрованного фрагмента. Видно, что количество «пройденных» тестов больше, нежели для незашифрованного фрагмента.

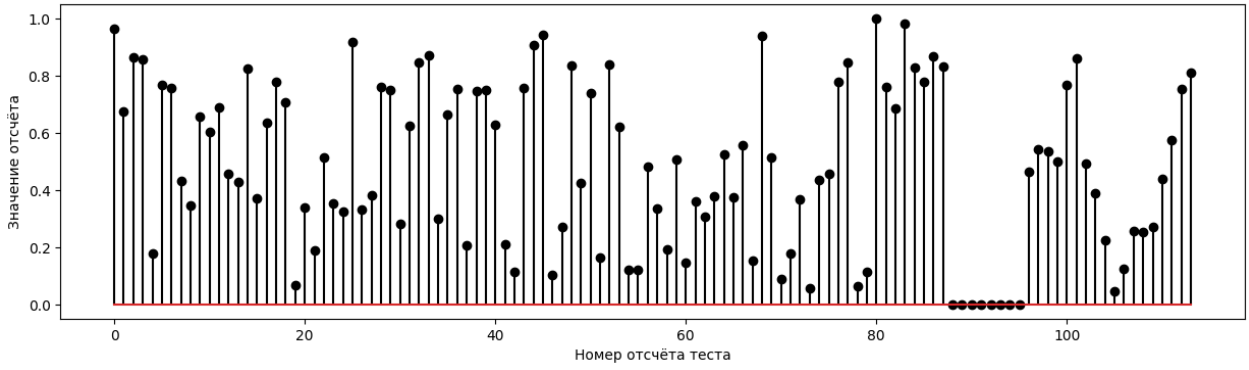


Рисунок 3.15 – Тест данных, зашифрованных Кузнечиком в режиме GCM

Сравнивая рисунки 3.13 и 3.15, содержащих статистические тесты зашифрованных фрагментов сложно сделать определенные выводы о «статистическом портрете» зашифрованного сообщения, за исключением того, что отсчеты результатов тестов имеют большие значения, в сравнении с отсчетами результатов тестов для незашифрованного сообщения. Таким образом, в качестве модели сообщения будем рассматривать три варианта последовательностей – незашифрованную, зашифрованную шифром AES и зашифрованную шифром Кузнечик.

3.3. Методика оценки последовательностей

Исследования показали, что ряд тестов, входящих стандарт NIST лишен смысла при анализе реальных данных. Так тест №7 «Тест на совпадение перекрывающихся шаблонов» и тест №9 «Тест на совпадение неперекрывающихся шаблонов» выявляют изъяны ГПСЧ и слабо связаны с потоком случайной информации в сети. Тест 10 «Тест на линейную сложность» направлен на выявление использование регистров с обратной связью в ГПСЧ, что не имеет смысла при анализе потока шифрованных данных. Некоторые тесты возвращают значительной количество отсчетов, что сильно запутывает задачу оценки. Рассмотрим алгоритм проведения исследований.

В качестве сообщения рассматривались данные из файла, рассмотренного в предыдущем параграфе. В качестве ПО рассмотрены 4 музыкальных фрагмента различных жанров, а именно: классика, два джазовых фрагмента и рок, представленные в виде отсчетов без сжатия. В качестве исходных данных использованы файлы формата FLAC.

Так как данные имеют тенденцию меняться, рассмотрение одного участка музыкального фрагмента недостаточно, поэтому проводилось 100 экспериментов со скачущим окном. Степень перекрытия окон выбрана равной половине окна. Рассмотрим процесс на примере первого теста. На рисунке 3.16 представлен результат тестирования с помощью первого теста скользящих окон незашифрованного фрагмента данных файла PDF. Размер окна 160 000 бит.

Визуальный анализ полученных результатов осложнен, поэтому использована гистограмма результатов. Гистограмма формируется из 10 диапазонов («корзин») и представлена на рисунке 3.17. Видно, что значительная часть результатов приходится на младший диапазон значений, что объясняется неравномерным распределением битов в незашифрованном файле. Аналогично проведен эксперимент для зашифрованных AES данных [69]. На рисунке 3.18 представлен результат первого теста по отсчетам для соответствующих окон, а на рисунке 3.19 гистограмма результатов первого теста.

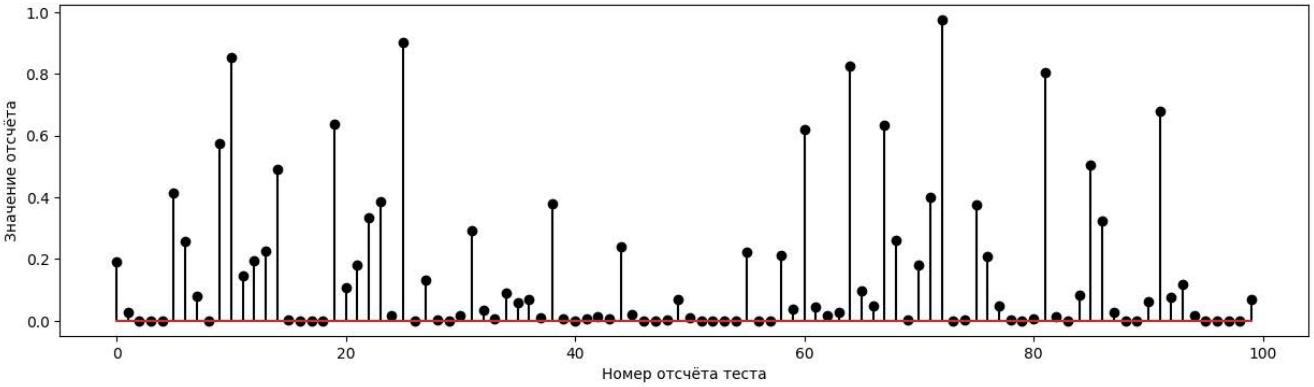


Рисунок 3.16 – Частотный побитовый тест незашифрованных данных

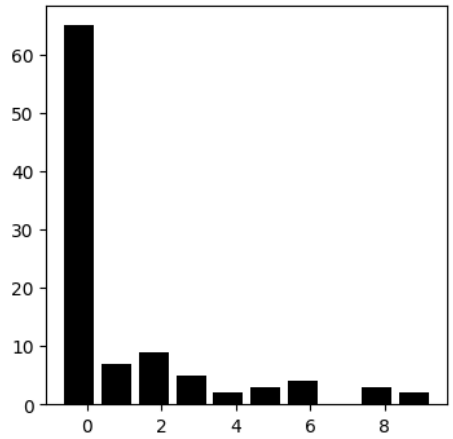


Рисунок 3.17 – Гистограмма результатов частотного побитового теста незашифрованных данных

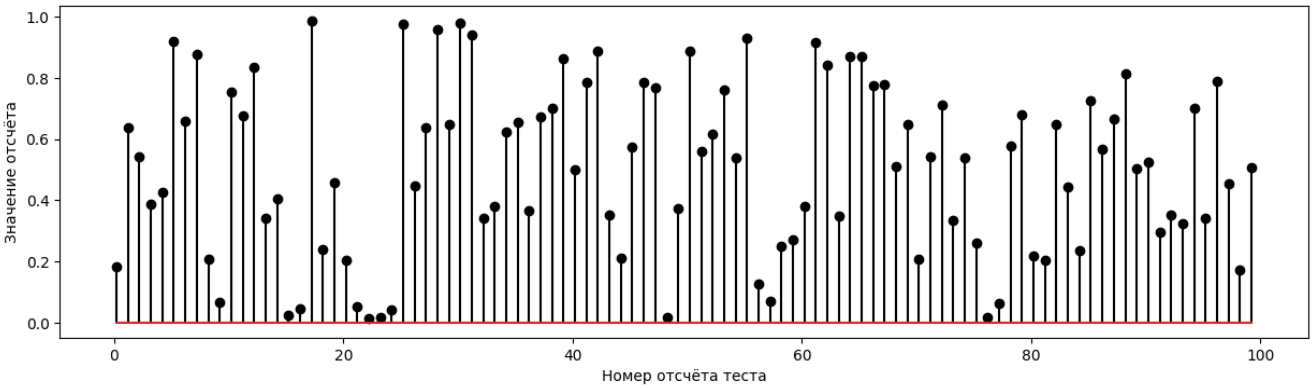


Рисунок 3.18 – Частотный побитовый тест зашифрованных AES данных

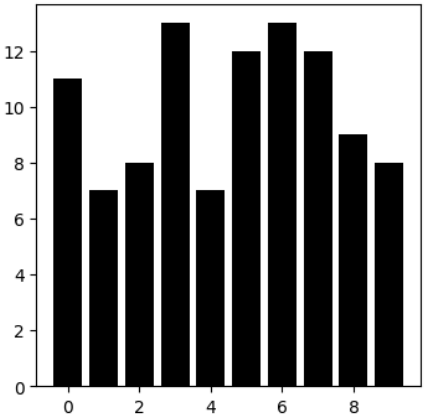


Рисунок 3.19 – Гистограмма результатов частотного побитового теста зашифрованных AES данных

Третий вариант сообщения использует шифрование отечественным шифром Кузнечик [7,42]. Результат теста зашифрованных данных представлен на рисунке 3.20, а гистограмма результатов на рисунке 3.21.

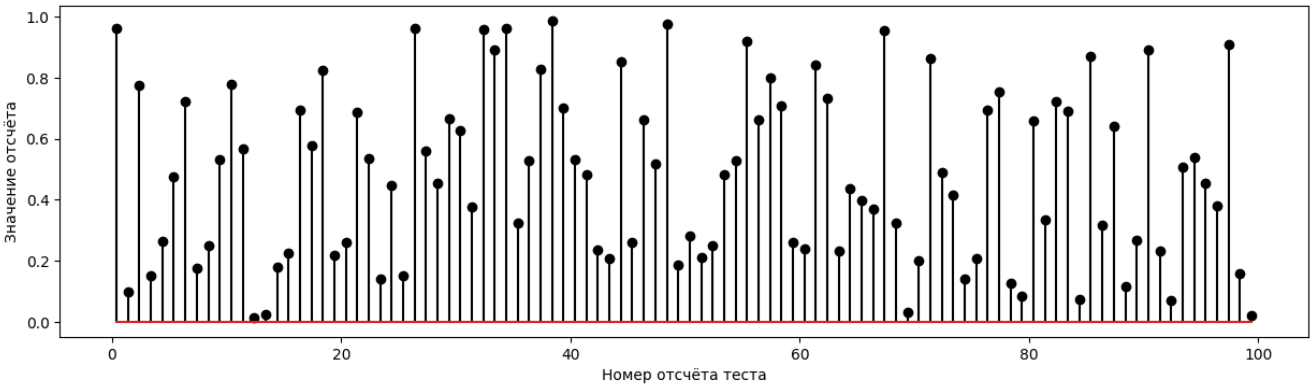


Рисунок 3.20 – Частотный побитовый тест зашифрованных Кузнечиком данных

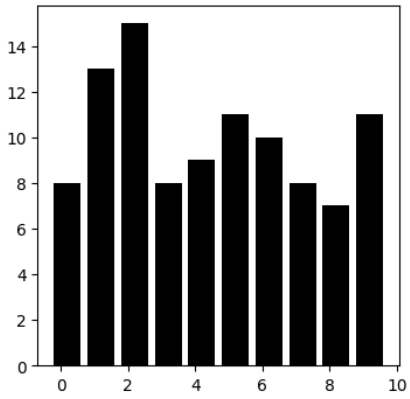


Рисунок 3.21 – Гистограмма результатов частотного побитового теста зашифрованных Кузнечиком данных

Сравним данные результаты с младшим битовым слоем звуковых фрагментов. Первый анализируемый фрагмент представляет собой симфоническое произведение одного из классиков. Произведение отличается мягким звучанием и отсутствием резких переходов и барабанов. На рисунке 3.22 представлен результат тестирования младшего битового слоя первого музыкального фрагмента первым тестом. Гистограмма построена для двух младших битовых слоев и представлена на рисунке 3.23. Младший битовый слой представлен столбцами, второй слой представлен отсчетами. Это сделано для сравнения статистических характеристик двух слоев. Можно увидеть, что статистически данный фрагмент значительно отличается как от незашифрованных данных, так и от зашифрованных. Между младшими слоями присутствует корреляционная связь.

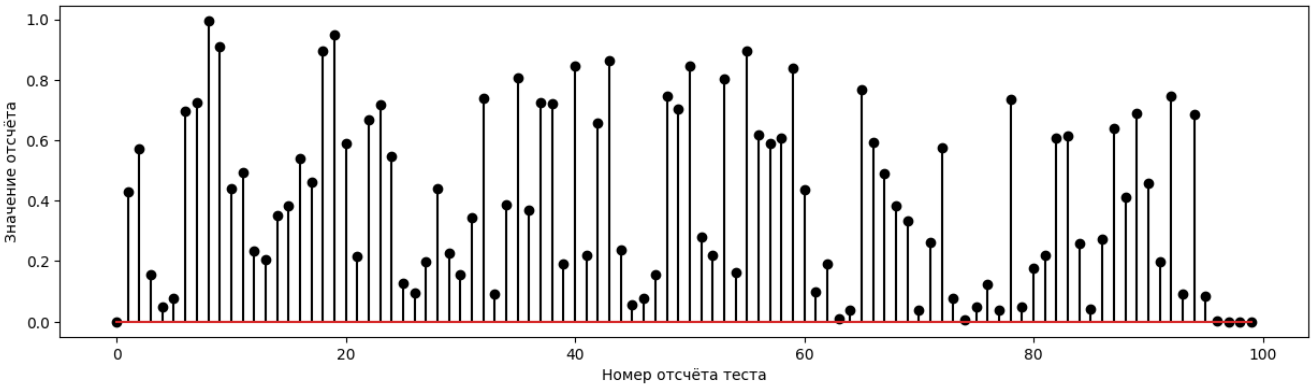


Рисунок 3.22 – Частотный побитовый тест первого музыкального фрагмента

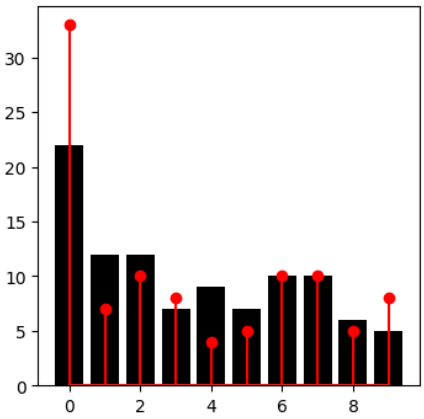


Рисунок 3.23 – Гистограмма результатов частотного побитового теста первого музыкального фрагмента

Рассмотрим второй (джазовый) фрагмент. Данный фрагмент содержит саксофонную партию и мягкие ударные. На рисунке 3.24 представлен результат тестирования младшего битового слоя второго музыкального фрагмента первым тестом. Гистограмма построена для двух младших битовых слоев и представлена на рисунке 3.25

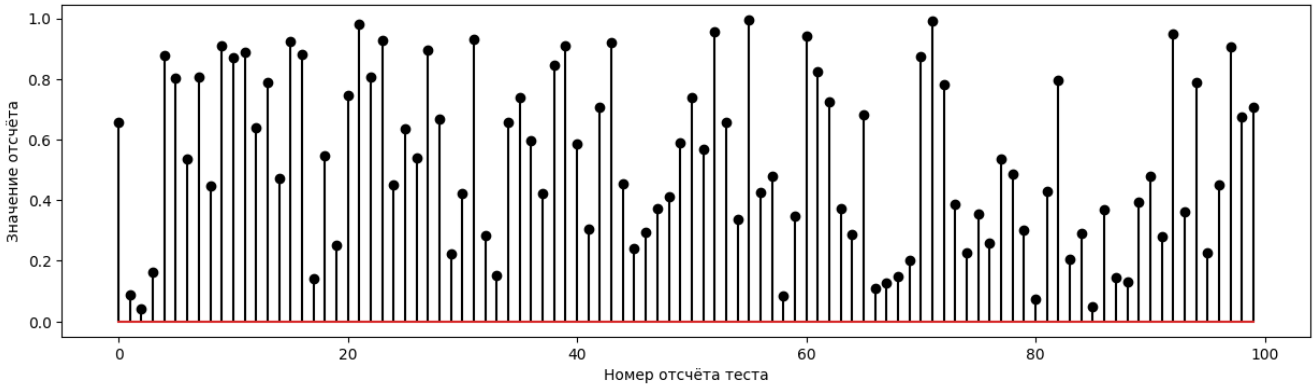


Рисунок 3.24 – Частотный побитовый тест второго музыкального фрагмента

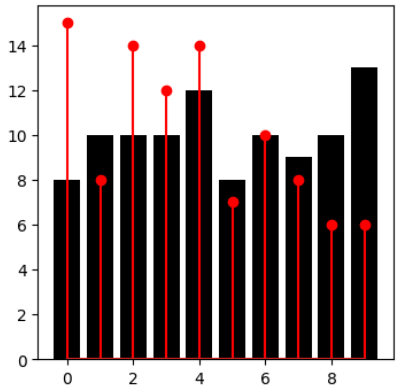


Рисунок 3.25 – Гистограмма результатов частотного побитового теста второго музыкального фрагмента

Видно, что у второго фрагмента, в соответствии с первым тестом, корреляция между младшими слоями мала. То есть, в зависимости от каждого, конкретного, фрагмента связь между слоями может как присутствовать, так и отсутствовать. Однако, присутствие связи не является аномальным, в то время как отсутствие связи может рассматриваться как наличие скрытой информации. В случае стегоанализа, если рассматривать отсутствие связи между слоями, как признак наличия скрытой информации, то в ряде случаев будет возникать ошибка первого рода.

Исследование показало, что из 15 тестов, входящих в состав NIST наиболее подходящими для оценки эффективности стеганографической системы, являются тесты:

Тест 1 – Частотный побитовый тест

Тест 2 – Частотный блочный тест

Тест 9 – Универсальный статистический тест Маурера

Тест 12 – Тест приблизительной энтропии

Тест 13 – Тест кумулятивных сумм (2 результата)

Методика оценки эффективности стегосистем базируется на анализе результатов тестов. Очевидно, что характер последовательности зашифрованных данных крайне сложно отличить от случайной последовательности, характерной для области младших битовых слоев покрывающего объекта типа изображение

или звук без сжатия. Однако, в случае коррелированности битовых слоев такое обнаружение возможно. Обратный эффект можно наблюдать для ПО со сжатием, где характер битовых последовательностей неслучаен, и зашифрованные данные могут быть обнаружены [19-20,58,70,75-76,84,87,108,110].

Проведем несколько проверок битовых последовательностей и проанализируем результаты. Для наглядности будем анализировать результаты выбранных тестов, примененных к каждому блоку данных. Чтобы не было пересечения с уже приведенными результатами, увеличим степень перекрытия до 90% и рассмотрим результаты для разного размера выборок.

Первый блок данных – незашифрованный PDF. На рисунке 3.26 приведены результаты тестирования блока размером 12500 байт (100 000 бит). Видно, что большая часть окон не проходит тест на случайность. Особенно хорошо это заметно по гистограммам, приведенным на рисунке 3.27. По гистограммам хорошо видно, что незашифрованные данные при анализе на случайность проваливают большую часть тестов, что приводит к тому, что первый столбец гистограммы (со значениями результатов тестов в диапазоне от 0 до 0,1) имеет наибольшее значение. Для данной проверки эффективны все тесты, однако тест 9 показывает наилучший результат.

Проведем исследование для окна размером 125000 байт (1 млн. бит). На рисунке 3.28 представлены результаты тестирования. На рисунке 3.29 представлены гистограммы результатов тестирования.

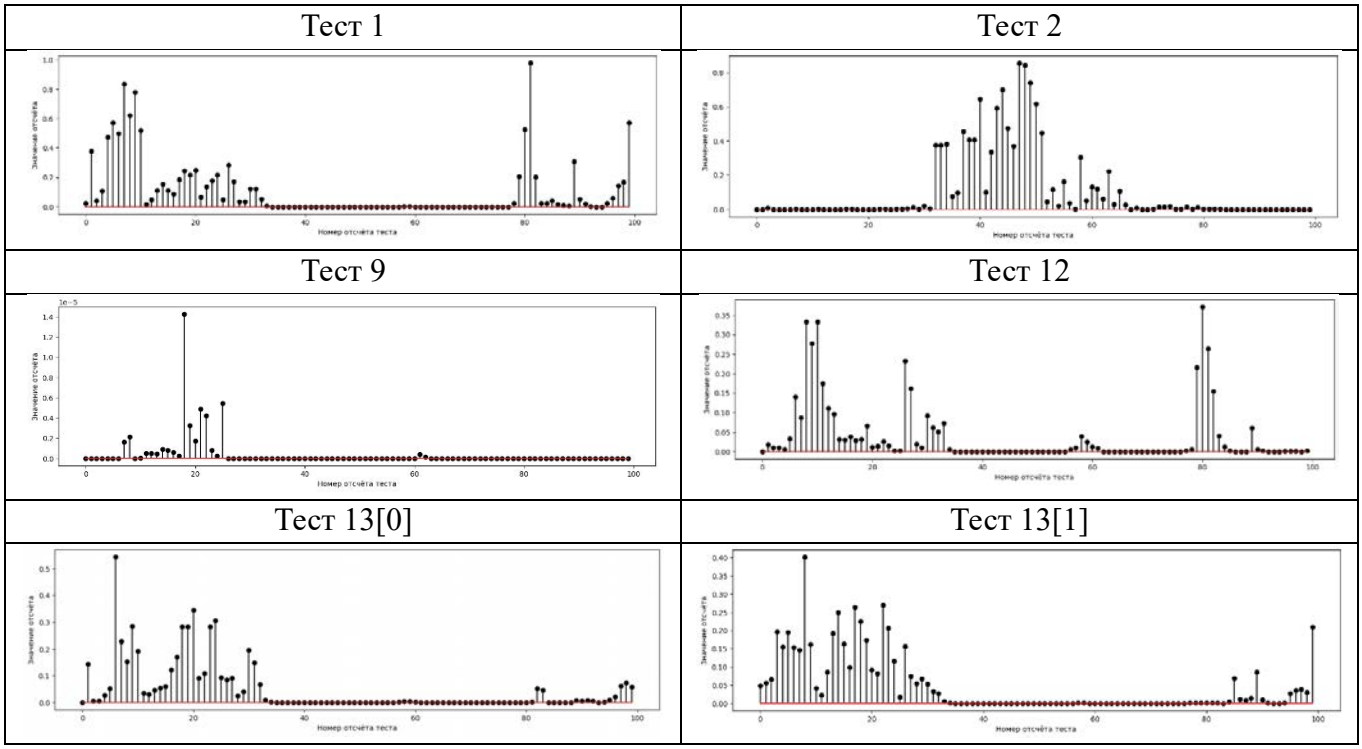


Рисунок 3.26 – Результаты тестирования незашифрованного блока данных 12500 байт (100 000 бит)

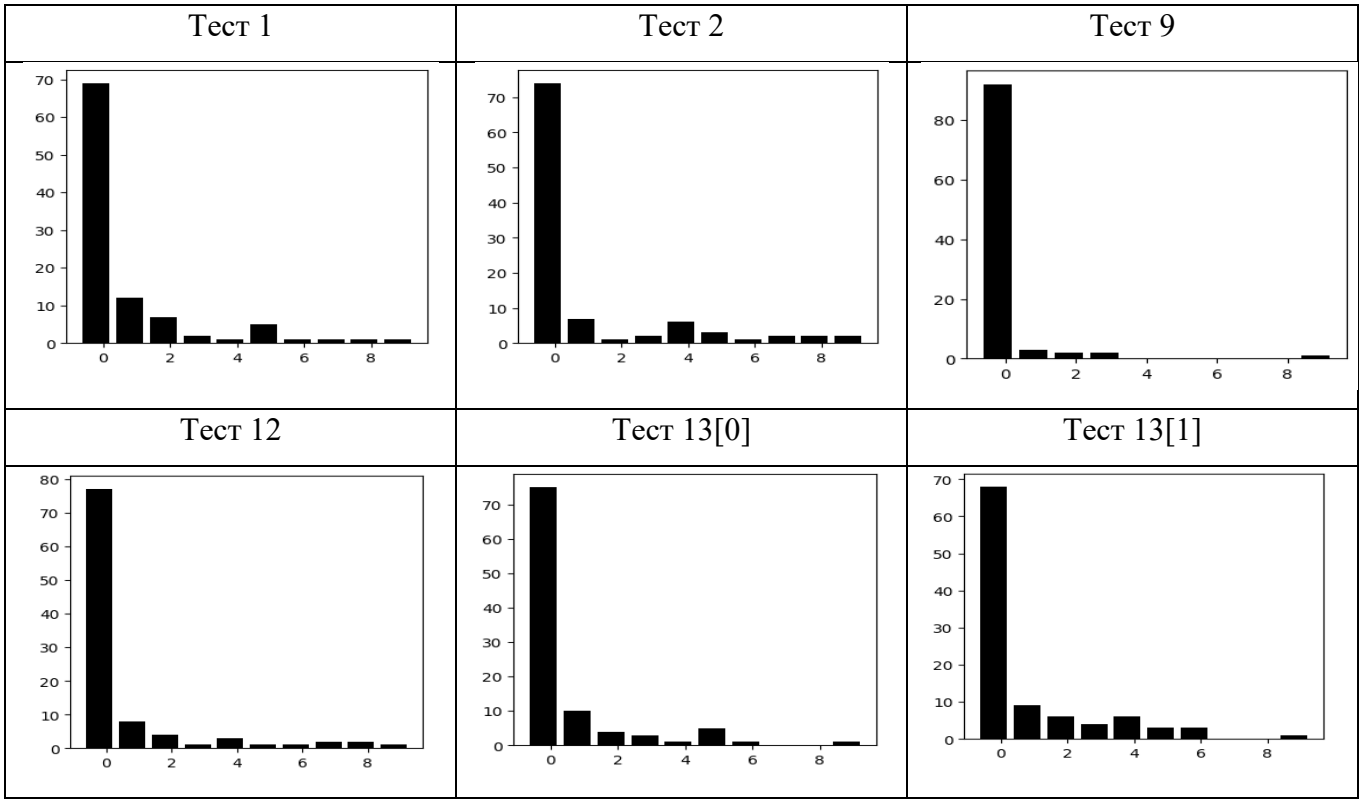


Рисунок 3.27 – Гистограммы результатов тестирования незашифрованного блока данных 12500 байт (100 000 бит)

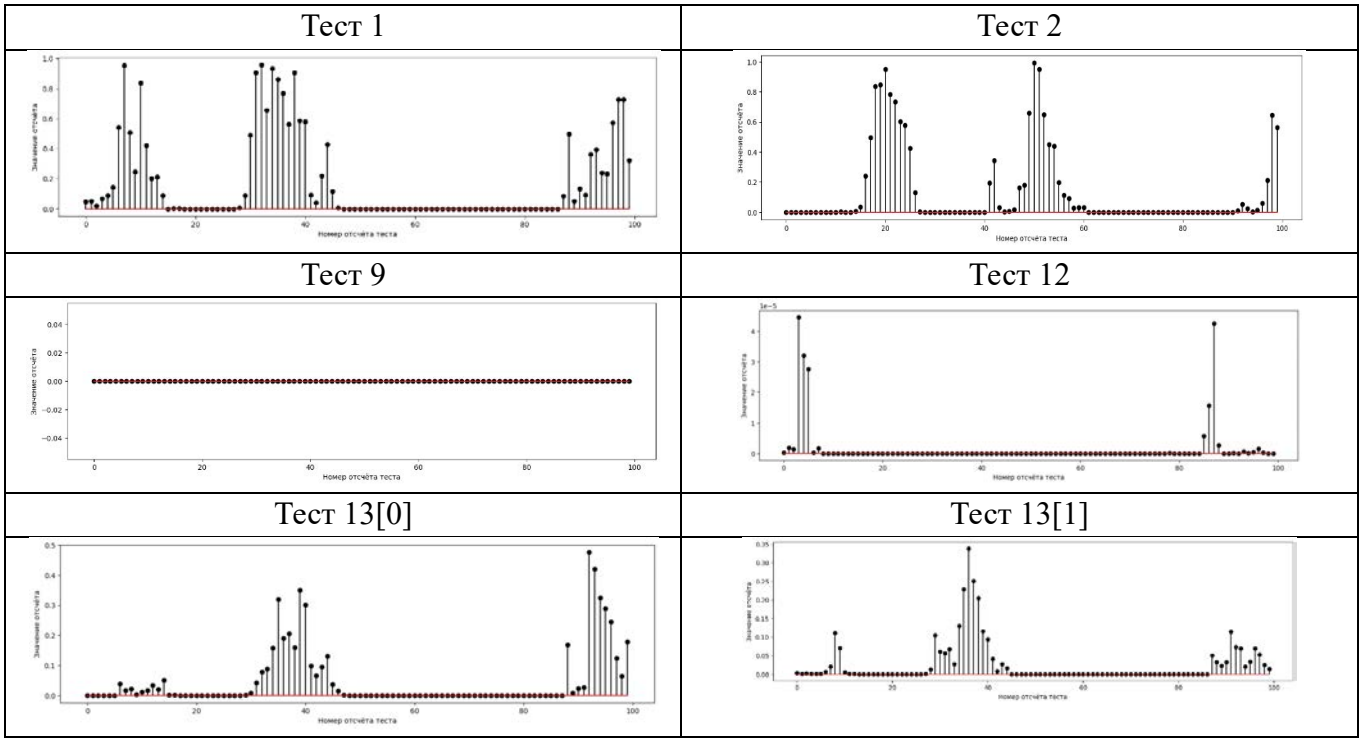


Рисунок 3.28 – Результаты тестирования незашифрованного блока данных 125000 байт (1 млн. бит)

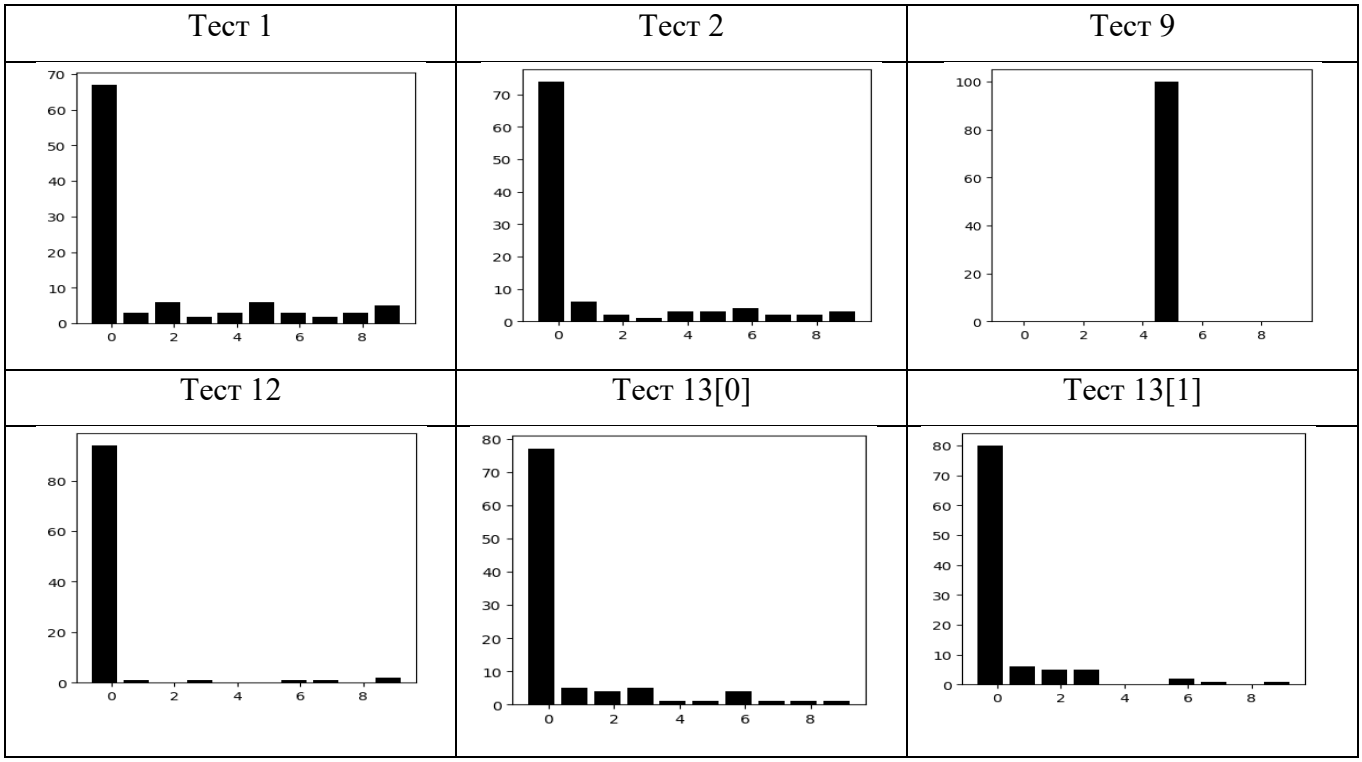


Рисунок 3.29 – Гистограммы результатов тестирования незашифрованного блока данных 125000 байт (1 млн. бит)

По результатам, приведенным на рисунках 3.26 – 3.29 можно сделать следующие выводы. Анализ больших последовательностей не вносит решающего значения в определение случайности, что можно увидеть по результату работы теста №9. Заметим, что при больших анализируемых последовательностях все универсальные статистические тесты Маурера были провалены. Однако при малой анализируемой последовательности гистограмма отличается незначительно. При этом время анализа увеличивается ощутимо. Важным моментом является охват значений. Тесты анализируют блоки разной длины, что привело к тому, что при тестировании больших последовательностей была задействована большая часть данных. С одной стороны – это хорошо, с другой – требует большего объема информации, что может быть ограничением, при анализе в реальном времени. Гистограммы, при этом, являются эффективным средством визуализации результатов.

Рассмотрим зашифрованный поток данных. На рисунке 3.30 приведены результаты тестирования блока, зашифрованного шифром AES размером 12500 байт (100 000 бит). На рисунке 3.31 приведены гистограммы результатов тестирования. Проведем исследование для окна размером 125000 байт (1 млн. бит). На рисунке 3.32 представлены результаты тестирования. На рисунке 3.33 представлены гистограммы результатов тестирования.

По результатам тестирования видно, что независимо от размера окна, большая часть тестов на случайность пройдены. Таким образом, зашифрованный фрагменты соответствуют случайным последовательностям, а выявление особенностей распределений результатов является вероятностной задачей, решение которой, в рамках данной работы, не ставится. Тем не менее, тот факт, что фрагменты звуковых файлов имеют участки пауз должен учитываться при встраивании, так как зашифрованные данные проходят тесты, а участки пауз в звуке их могут и не пройти.

Сравним полученные результаты с результатами анализа сообщения, зашифрованного шифром Кузнечик.

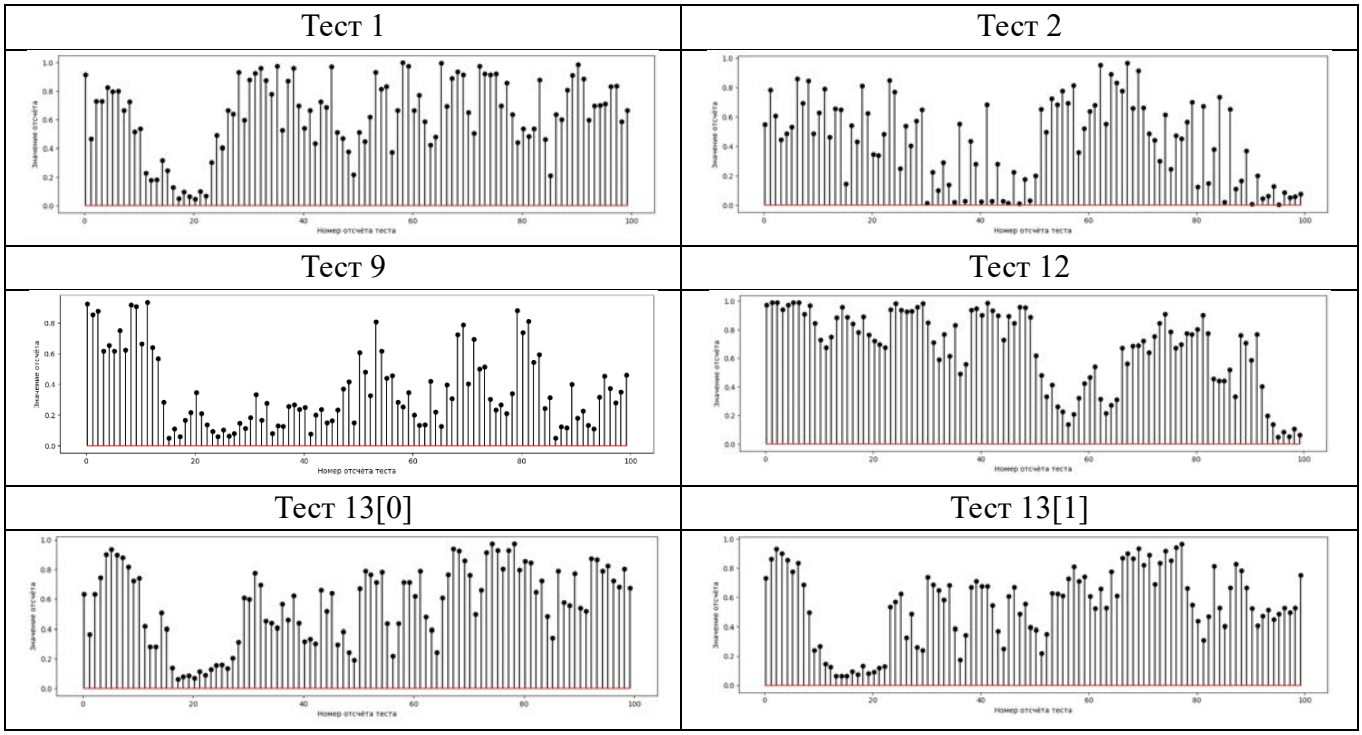


Рисунок 3.30 – Результаты тестирования, зашифрованного шифром AES блока данных 12500 байт (100 000 бит)

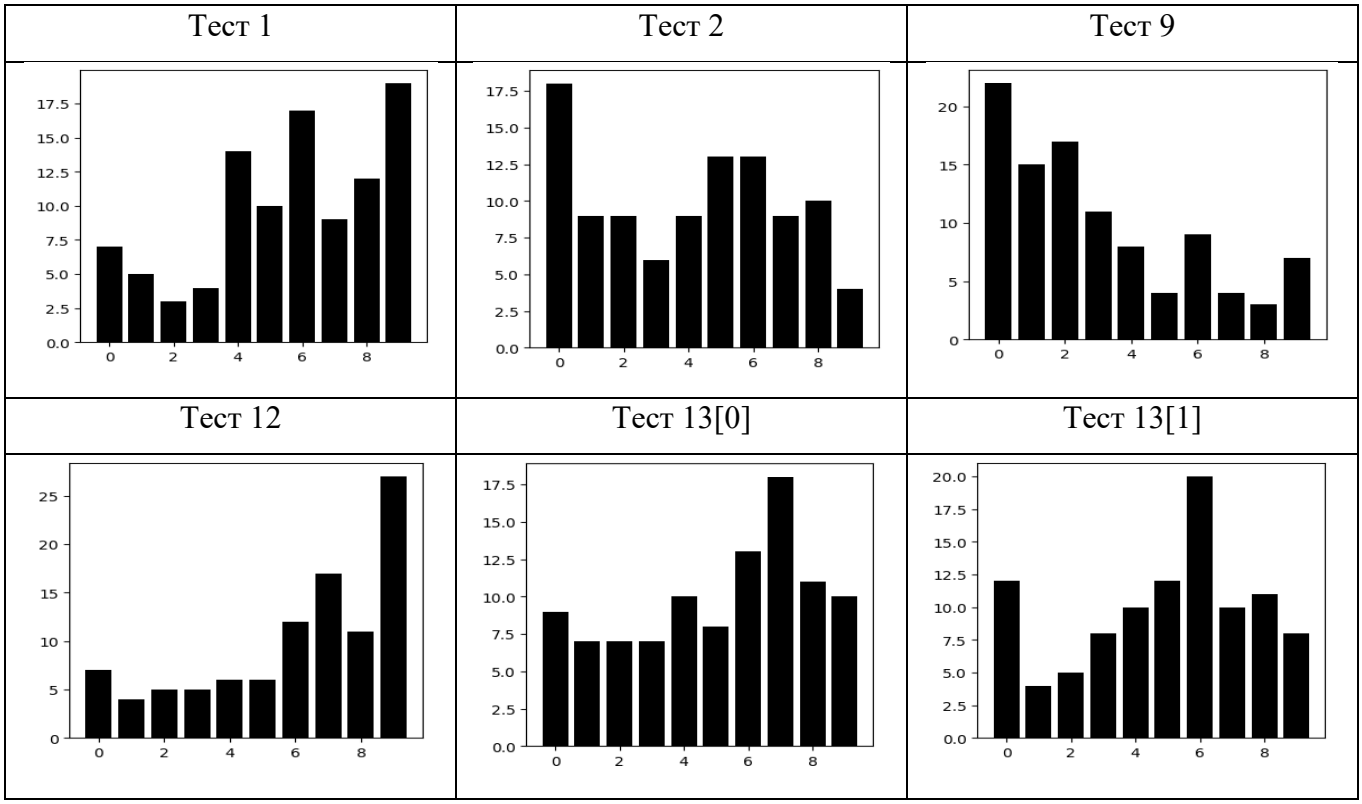


Рисунок 3.31 – Гистограммы результатов тестирования зашифрованного шифром AES блока данных 12500 байт (100 000 бит)

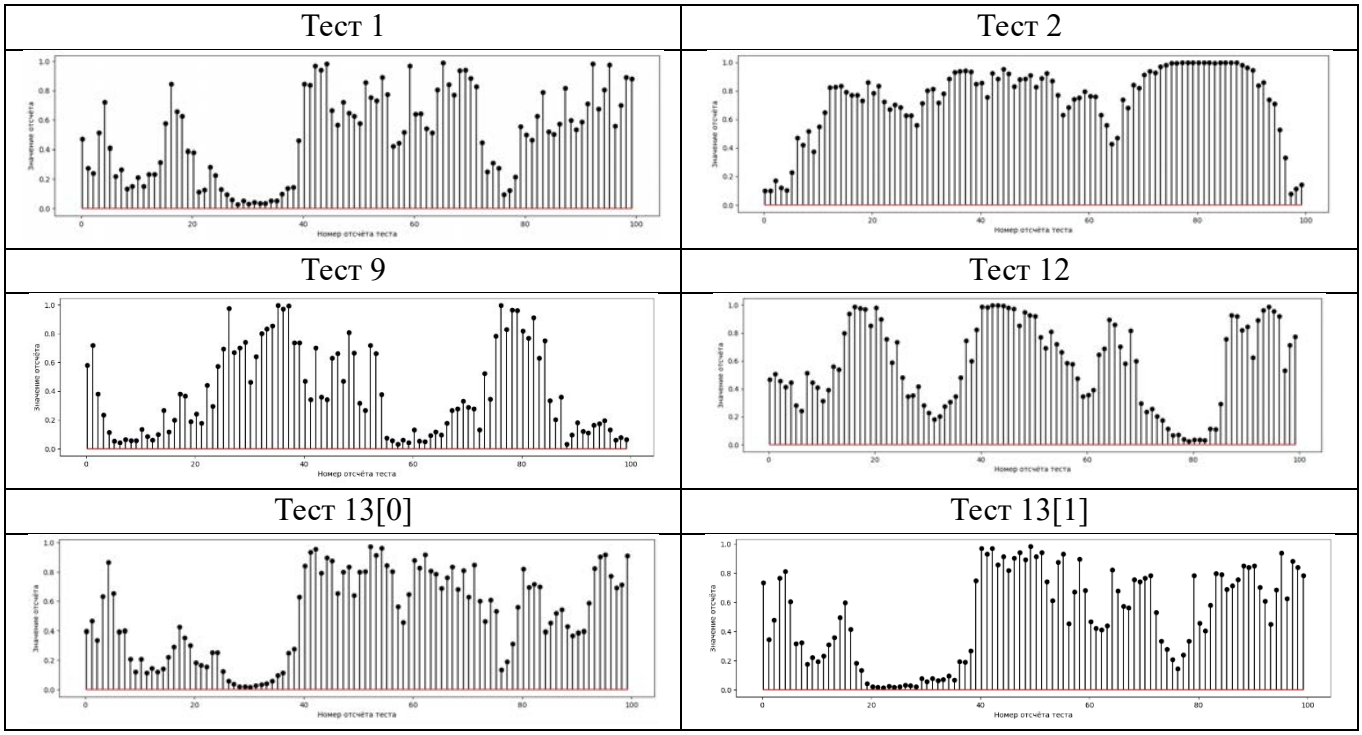


Рисунок 3.32 – Результаты тестирования, зашифрованного шифром AES блока данных 125000 байт (1 млн. бит)

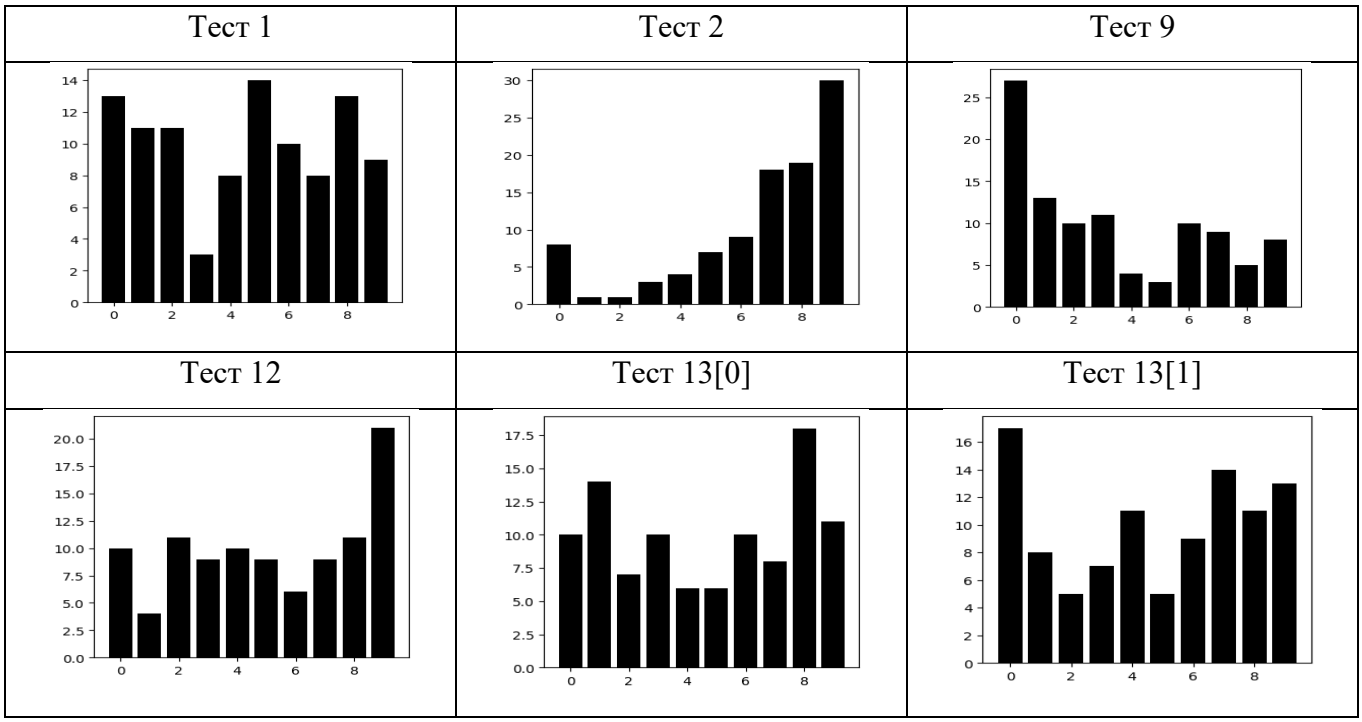


Рисунок 3.33 – Гистограммы результатов тестирования, зашифрованного шифром AES, блока данных 125000 байт (1 млн. бит)

На рисунке 3.34 приведены результаты тестирования блока, зашифрованного шифром «Кузнечик» размером 12500 байт (100 000 бит). На рисунке 3.35 приведены гистограммы результатов тестирования.

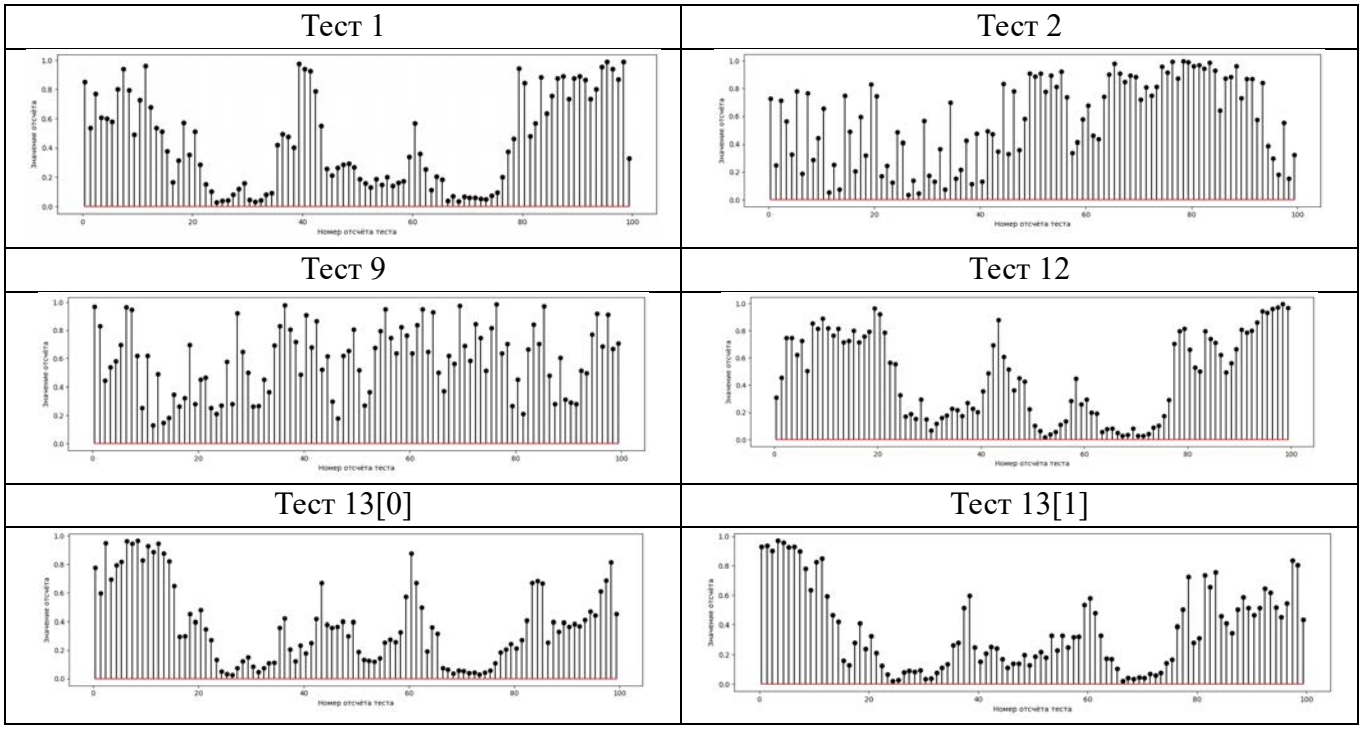


Рисунок 3.34 – Результаты тестирования блока, зашифрованного шифром «Кузнечик» размером 12500 байт (100 000 бит)

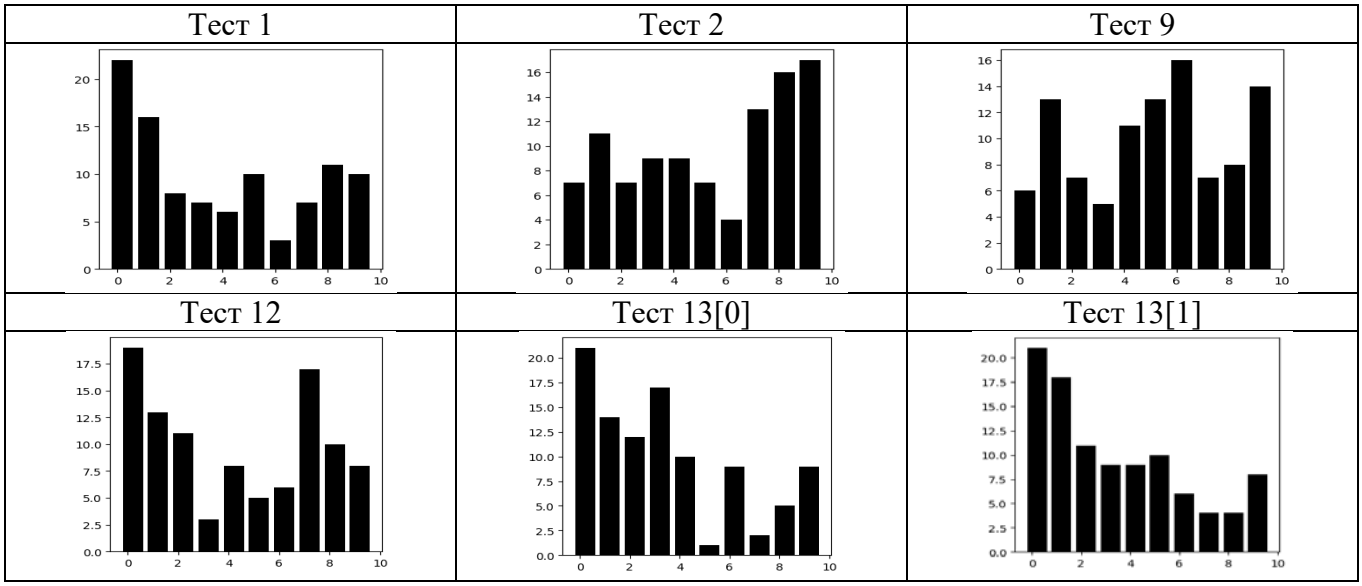


Рисунок 3.35 – Гистограммы результатов тестирования, зашифрованного шифром «Кузнечик» размером 12500 байт (100 000 бит)

Проведем эксперимент для окна размером 125000 байт (1 млн. бит). На рисунке 3.36 представлены результаты тестирования. На рисунке 3.37 представлены гистограммы результатов тестирования.

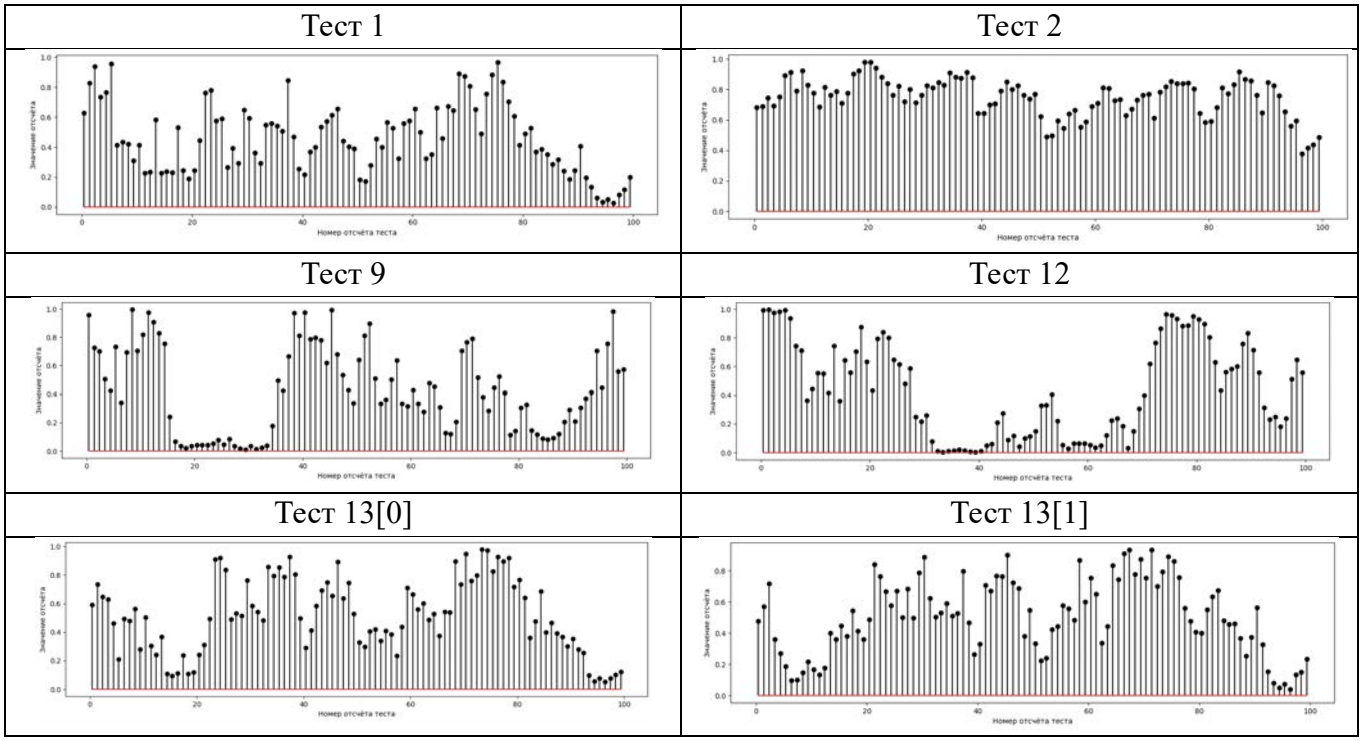


Рисунок 3.36 – Результаты тестирования блока, зашифрованного шифром «Кузнечик» размером 125000 байт (1 млн. бит)

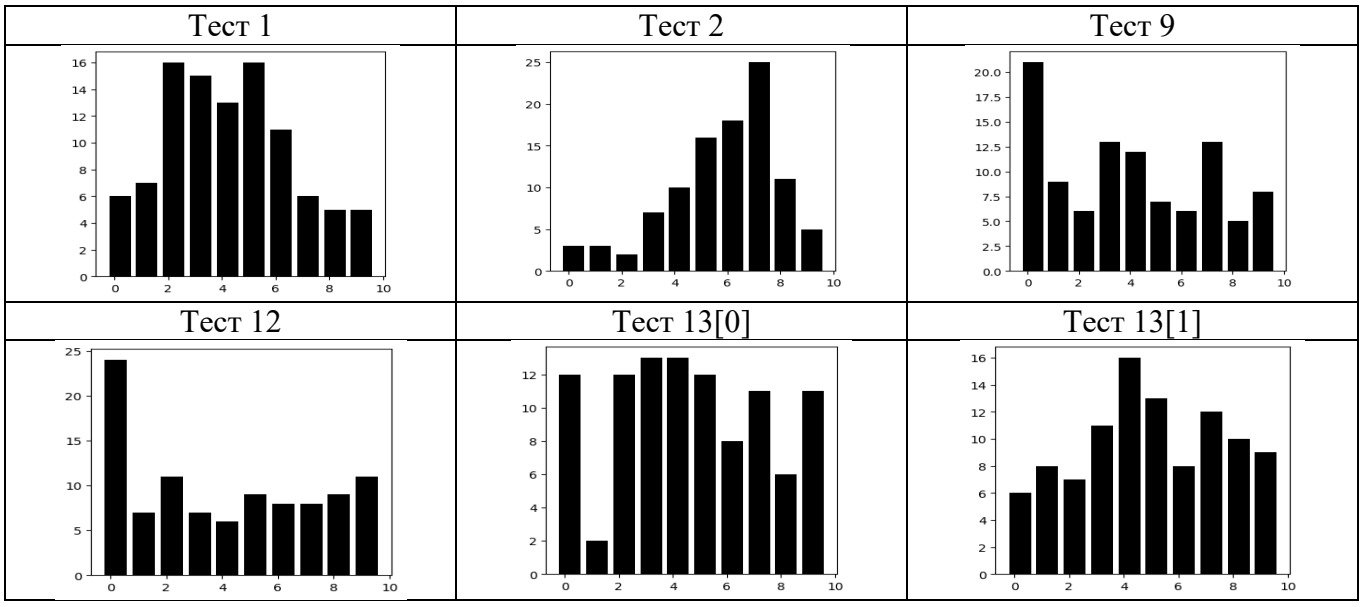


Рисунок 3.37 – Гистограммы результатов тестирования, зашифрованного шифром «Кузнечик», размером 125000 байт (1 млн. бит)

По полученным результатам можно сделать ряд выводов. Данные, зашифрованные шифром «Кузнечик» проходят тесты на случайность. Изменение окна оказывает значительное влияние на результат тестов. Так тест №2 при увеличении окна начинает стабильно проходиться, в то время как тесты №9 и №12 имеют области, где результат теста имеет низкое значение. Очевидно, что использование тестов дает вероятностный результат, анализ которого должен идти в сравнении с результатом тестирования битовых слоев. Проведем тесты звуковых фрагментов. Так как объем полученных результатов достаточно велик, ограничимся приведением наиболее интересных результатов, на основе которых будут сделаны выводы.

Рассмотрим результаты статистического анализа первого (классического) музыкального фрагмента. На рисунке 3.38 приведен результат анализа выбранными тестами музыкального фрагмента с выбранным размером окна 12500 байт. Можно увидеть большое количество отсчетов с нулевыми значениями. Это продиктовано паузами в записи фрагментов.

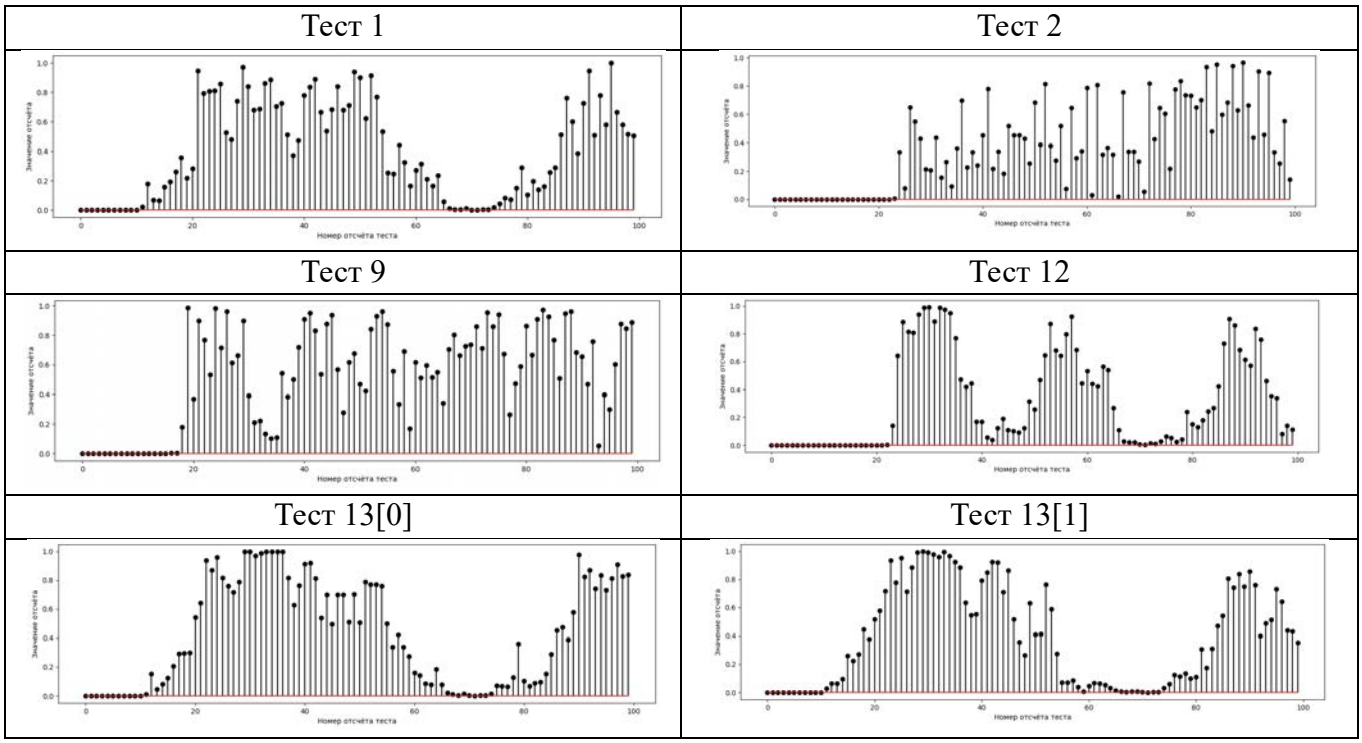


Рисунок 3.38 – Результаты тестирования первого музыкального фрагмента с размером окна 12500 байт

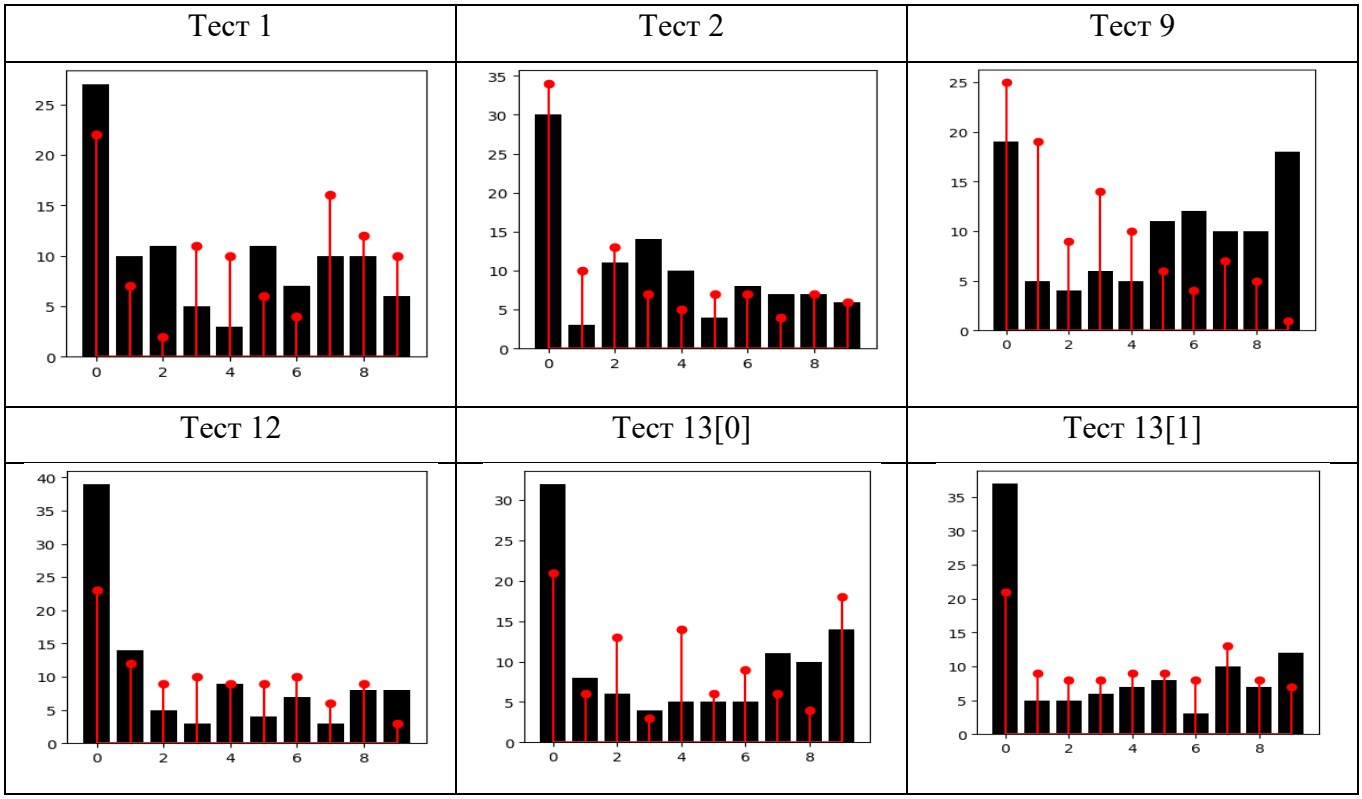


Рисунок 3.39 – Гистограммы результатов тестирования первого музыкального фрагмента с размером окна 12500 байт

На рисунке 3.39 приведены результаты тестов для первого фрагмента с выбранным размером окна 12500 байт. На рисунке 3.40 приведены гистограммы результатов тестирования второго музыкального фрагмента. Проанализируем результаты. По гистограммам на рисунке 3.41 видно, что большое количество тестов дают невысокие значения и попадают в первую корзину. При этом, увеличение размера выборки только усилило данный эффект. Однако, увеличение размера выборки нивелировало наличие небольших пауз в музыкальном фрагменте. Очевидно, что чем меньше окно выборки, тем сильнее проявляется коррелированность областей с паузами и тестов, дающих нулевой результат. Однако, сравнивая данный фрагмент с другими музыкальными фрагментами становится ясно, что при отсутствии выраженных пауз области отсчетов, дающих в результате тестирования нулевые результаты - пропадают. Так как три остальных фрагмента дают, качественно, похожий результат, приведем только один из них.

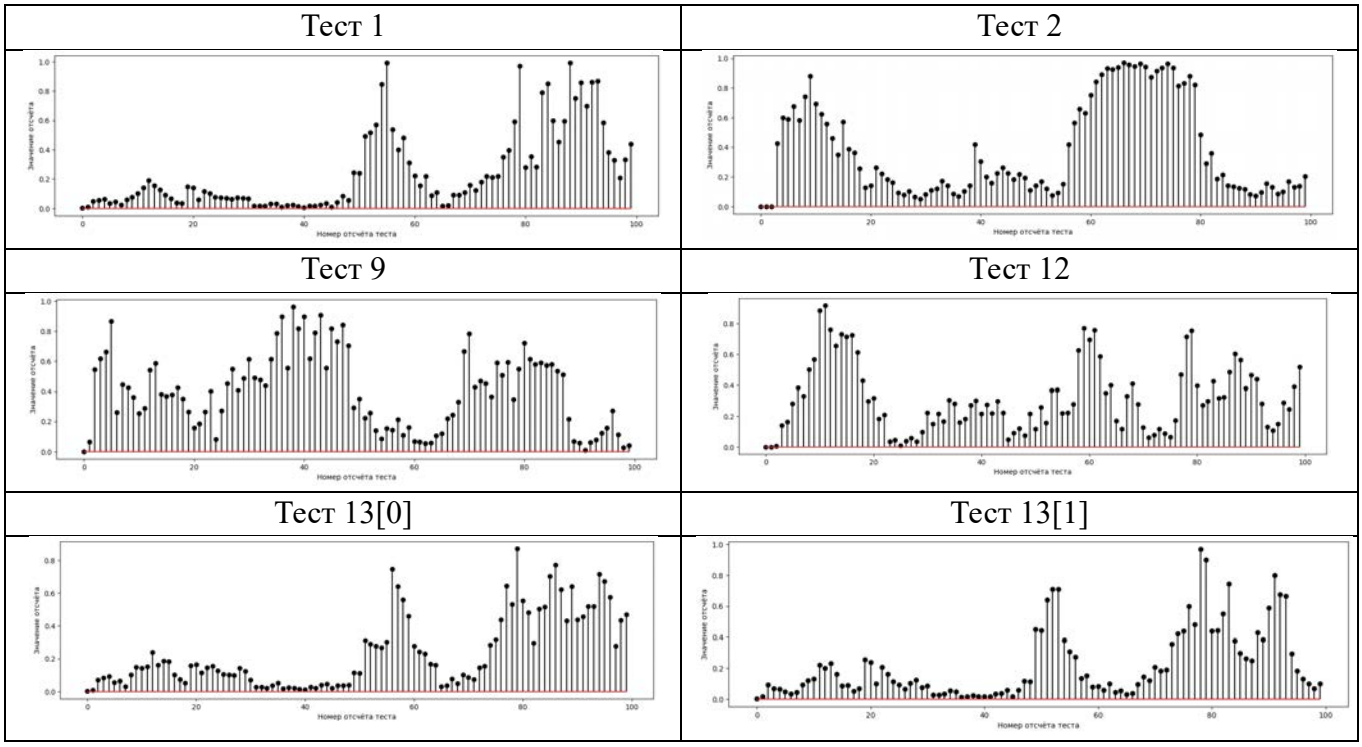


Рисунок 3.40 – Результаты тестирования второго музыкального фрагмента

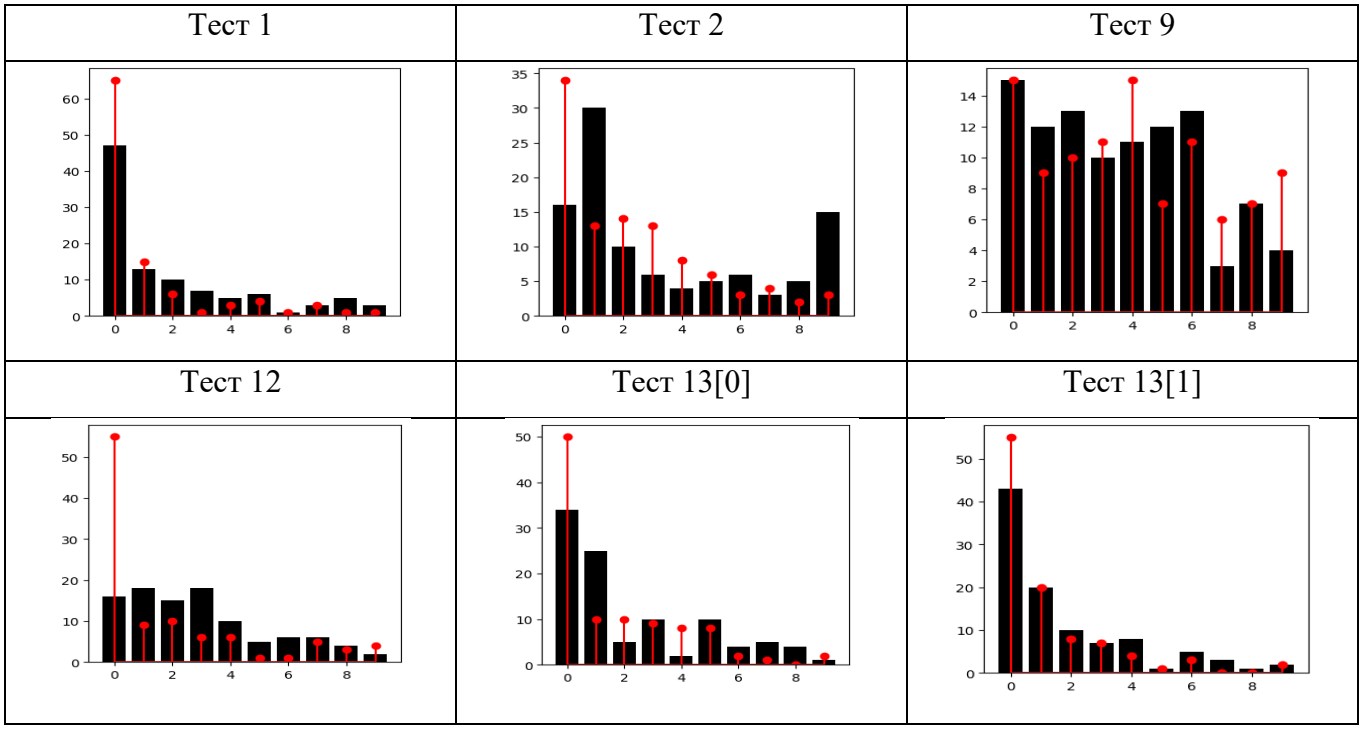


Рисунок 3.41 – Гистограммы результатов тестирования второго музыкального фрагмента

На рисунке 3.42 приведен результат тестирования третьего музыкального фрагмента с окном выборки 12500 байт. На рисунке 3.43 приведены гистограммы результата тестирования третьего музыкального фрагмента.

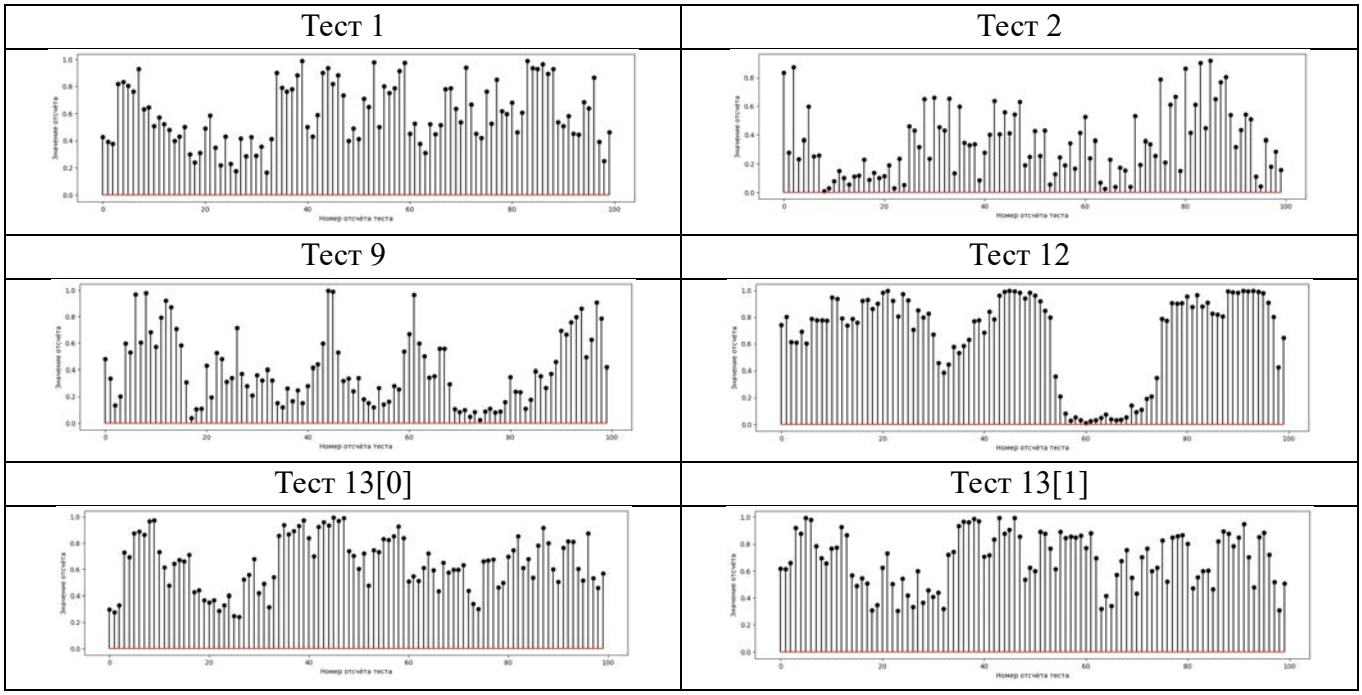


Рисунок 3.42 – Результаты тестирования третьего музыкального фрагмента с окном выборки 12500 байт

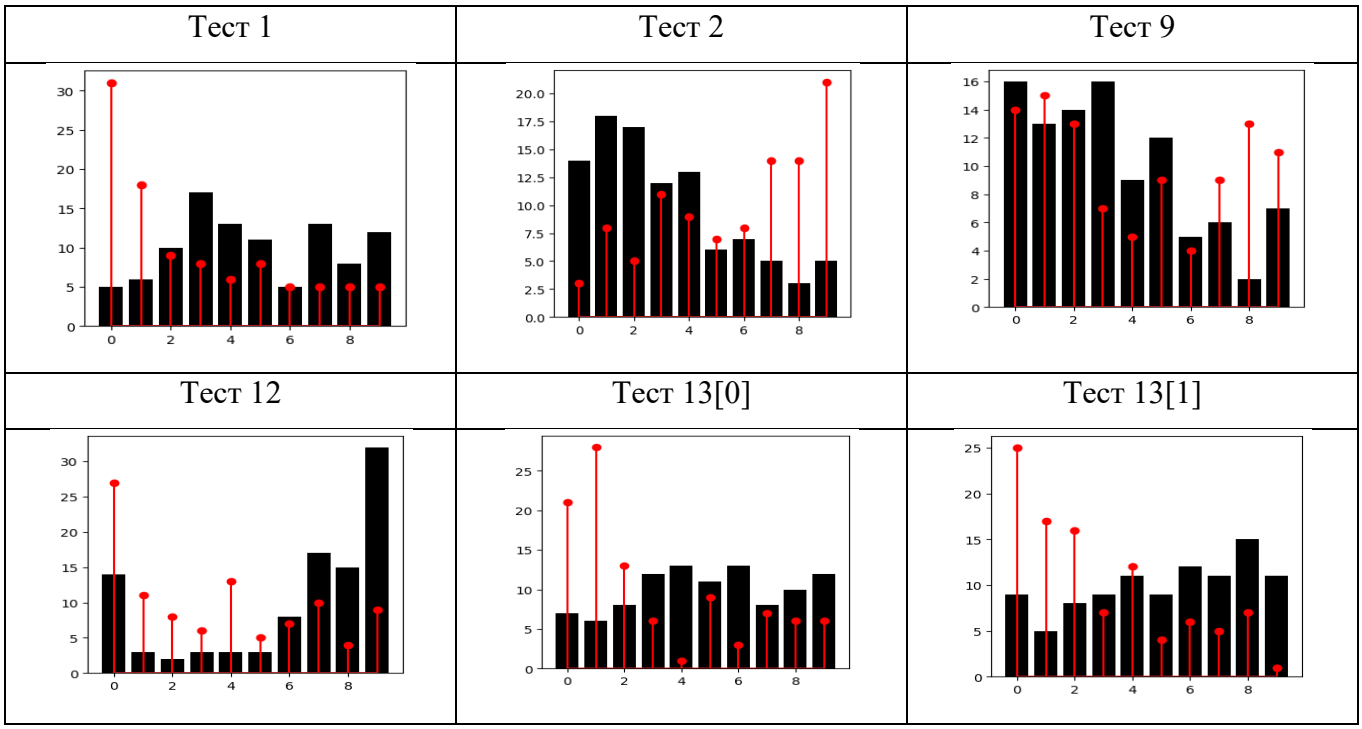


Рисунок 3.43 – Гистограммы результатов тестирования третьего музыкального фрагмента с окном выборки 12500 байт

Видно, что отсутствие пауз приводит к отсутствию областей с рядом подряд идущих фрагментов, проваливающих тесты. Причем, сравнивая данные результаты с результатами, приведенными на рисунках 3.30 и 3.34 (анализ зашифрованных блоков данных) можно сделать вывод, что статистическое обнаружение зашифрованных фрагментов в младшем битовом слое звукового сигнала без сжатия практически невозможно, если не задействуются области с паузами в звуковом сигнале.

Проанализируем результат, в случае окон выборки 125000 байт. На рисунке 3.44 приведен результат тестирования третьего музыкального фрагмента. На рисунке 3.45 приведены гистограммы результата тестирования третьего музыкального фрагмента. По рисункам видно, что выделить статистические отличия между результатами анализа зашифрованных фрагментов сообщения и младших битовых слоев не получается. Таким образом, использование зашифрованных сообщений является эффективным средством маскировки сообщений в младших битовых слоях.

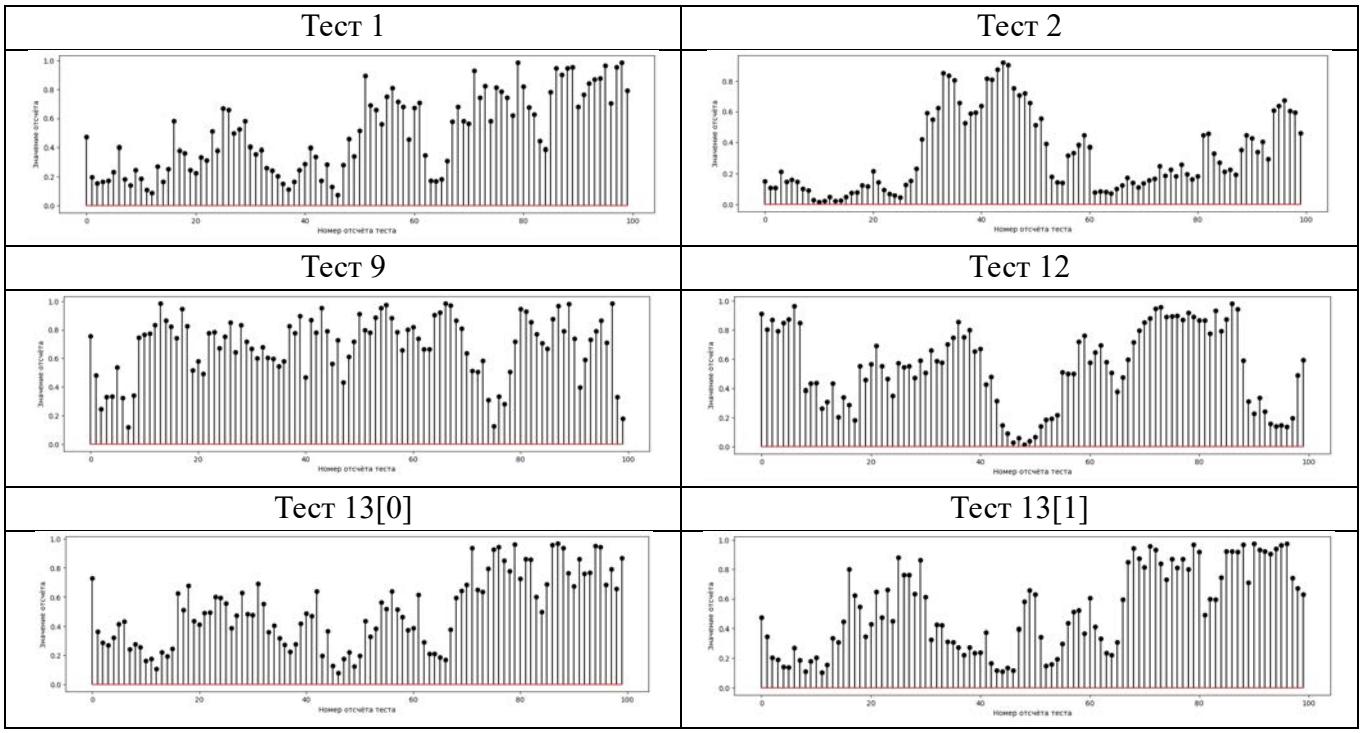


Рисунок 3.44 – Результаты тестирования третьего музыкального фрагмента с окном выборки 125000 байт

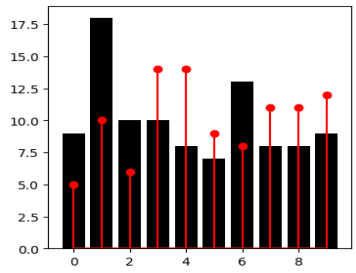
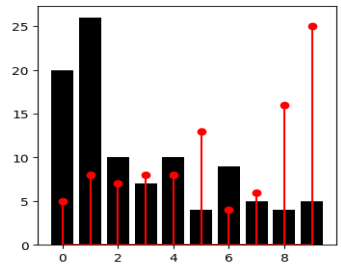
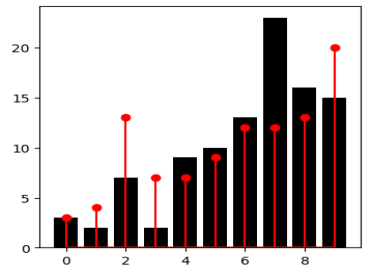
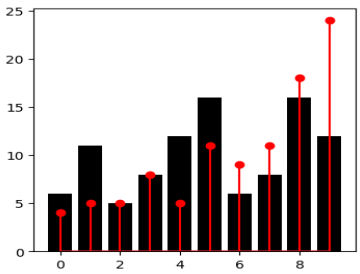
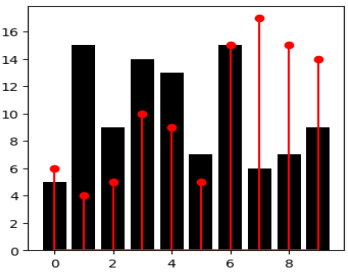
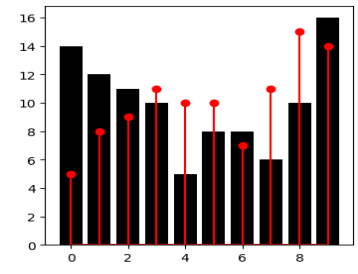
Тест 1	Тест 2	Тест 9
		
Тест 12	**Тест 13[0]**	**Тест 13[1]**
		

Рисунок 3.45 – Гистограммы результатов тестирования третьего музыкального фрагмента с окном выборки 125000 байт

Выводы по третьей главе

В главе предложена форма представления сообщения в виде незашифрованного потока бит и зашифрованного потока бит. Данный выбор обусловлен тем фактом, что если подбирать статистически «удобные» данные под заданные ситуации, то результат будет ярким, но не соответствующим реальности. С этой целью сформирован блок данных на основе реального файла типа PDF, содержащего текст и рисунки. Сообщение представляется совокупностью трех составляющих: незашифрованное сообщение, сообщение, зашифрованное шифром AES и сообщение, зашифрованное шифром «Кузнечик». В этом случае можно сравнить степень маскировки зашифрованных и незашифрованных сообщений в различных покрывающих объектах с помощью различных статистических инструментов. Для анализа предложены несколько тестов, входящих в стандарт NIST для анализа битовых последовательностей. Тесты выбраны на основе результатов анализа представленного сообщения и, в общем случае, могут быть использованы как указанные в главе тесты, так и другой их набор.

Проведенный анализ показал, что обнаружение зашифрованных фрагментов в области младших значащих бит звукового сигнала без сжатия проблематично, так как отсутствует выраженная корреляция между битовыми слоями сообщения, а младший битовый слой и зашифрованные фрагменты сообщения имеют статистический характер близкий к случайному.

Тем не менее, предложенный подход, использующий несколько NIST тестов является более информативным инструментом по сравнению с распространенной дивергенции Кульбака-Лейблера, сравнивающей распределения значений бит.

4. Исследование свойств стеганографических систем

Основной задачей данной главы является исследование свойств двухкомпонентных стеганографических систем для звуковых покрывающих объектов с помощью численных моделей, построенных на языке Python и определение наиболее эффективных алгоритмов формирования функций связи компонент для встраивания сообщений в звуковой ПО без использования сжатия. При построении численных моделей использован тестовый звуковой сигнал, представленный в ИКМ (формат WAVE). В качестве образцов используем звуковые сигналы из третьей главы. Согласно методикам, изложенным в [79,98], выбор тестовых фрагментов различных жанров (классика, джаз, рок) позволяет оценить универсальность стеганографических алгоритмов. Рассмотрим различные варианты формирования функций связи компонент, и проведем оценку маскировки при использовании различных алгоритмов встраивания.

Исходя из того, что во всех моделях будем использовать одинаковые ПО, использованные в третьей главе, проведем их предварительный анализ. В третьей главе анализ ПО частично уже был проведен при демонстрации статистических методов, поэтому здесь проведем его целенаправленно, для определения ключевых свойств ПО. Под ключевыми свойствами нас интересует степень коррелированности слоев, а также области нулевого сигнала и области максимального сигнала. Заметим, что последние в музыкальных фрагментах, как правило, не встречаются. Тем не менее, если такая область присутствует, то встраивание в эту область не рекомендуется, такая область может быть обнаружена.

4.1. Исследование свойств покрывающих объектов

Первой задачей встраивания двухкомпонентного контейнера, использующего в качестве первой компоненты бит старшего слоя, является определение слоев, из которых первая компонента извлекается. Очевидно, что чем старше битовый слой, тем больше он коррелирован с информацией ПО. В

случае изображений возможен визуальный анализ. Однако, с точки зрения статистики можно воспользоваться статистическими тестами, определяющими случайность последовательности. Если последовательность случайна, значит ее можно считать некоррелированной и слой приемлемым для извлечения первой компоненты. Проведем анализ по слоям.

Первый тест, входящий состав NIST тестов анализирует распределение значений. Проведем проверку всех битовых слоев первого музыкального фрагмента [4]. На рисунке 4.1 приведены гистограммы распределений результатов тестирования скользящих блоков с перекрытием в 90% окна. На рисунке приведены только результаты по младшим 8 слоям. Начиная с 8-ого слоя все тесты проваливаются, то есть результаты тестов 8-16 идентичны. Поэтому результаты для слоев 9-16 на рисунке не приведены.

Проведем проверку вторым тестом первого музыкального фрагмента. Результат приведен на рисунке 4.2. Видно, что слои, не проходящие тест №2 аналогичны тесту №1.

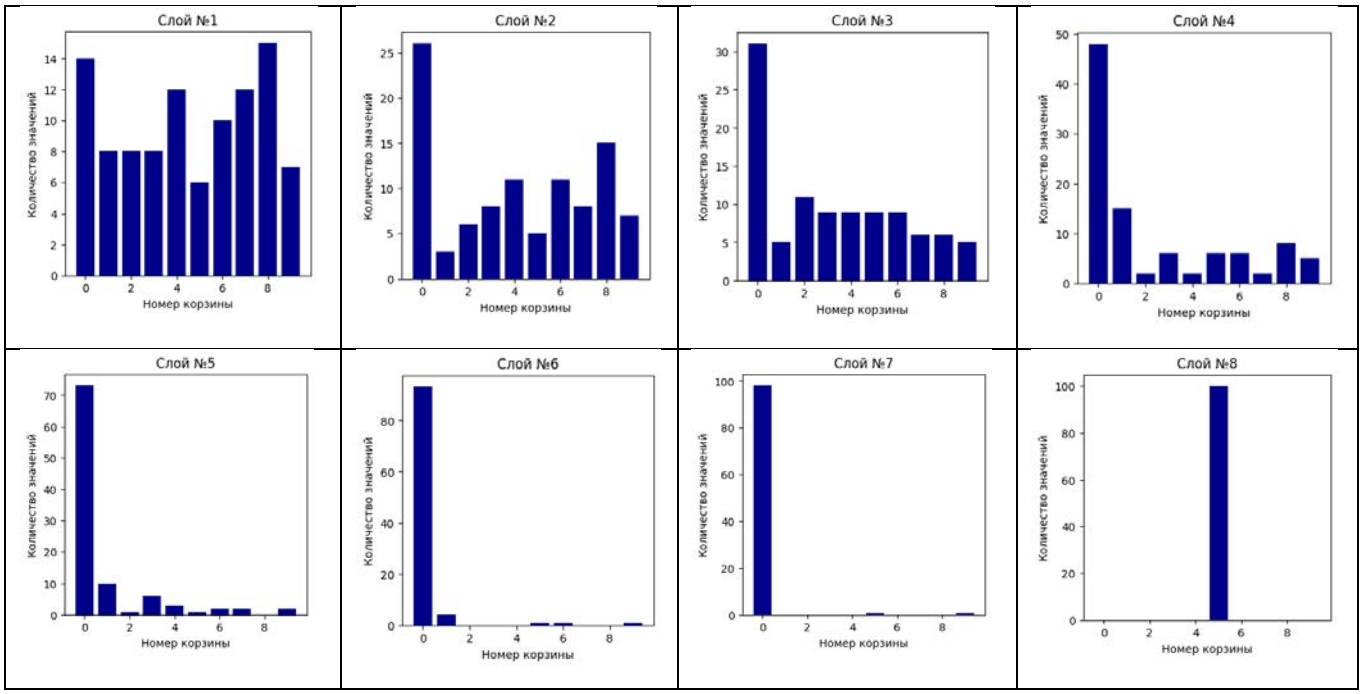


Рисунок 4.1 – Распределения значений результатов первого NIST теста слоев первого ПО

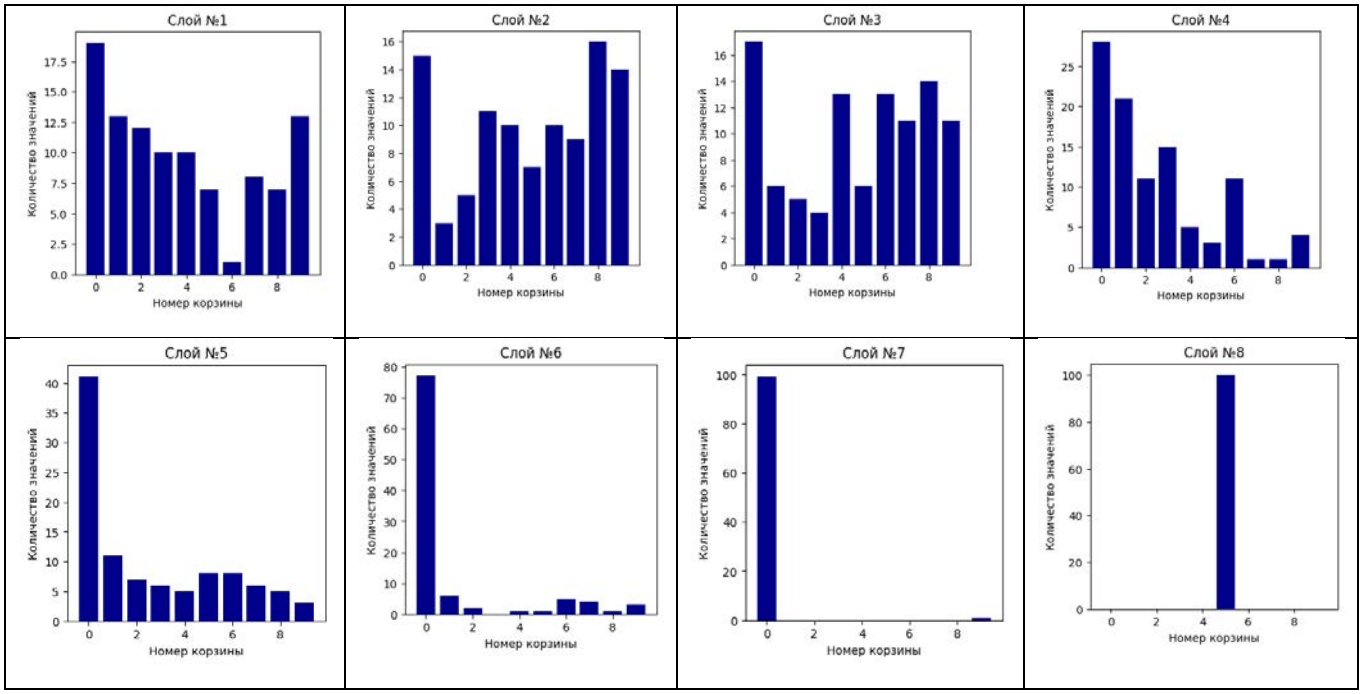


Рисунок 4.2 – Распределения значений результатов второго NIST теста слоев первого ПО

Проведем тестирование тестами №9 и №12. На рисунках 4.3 и 4.4 приведены, соответственно, результаты тестирования.

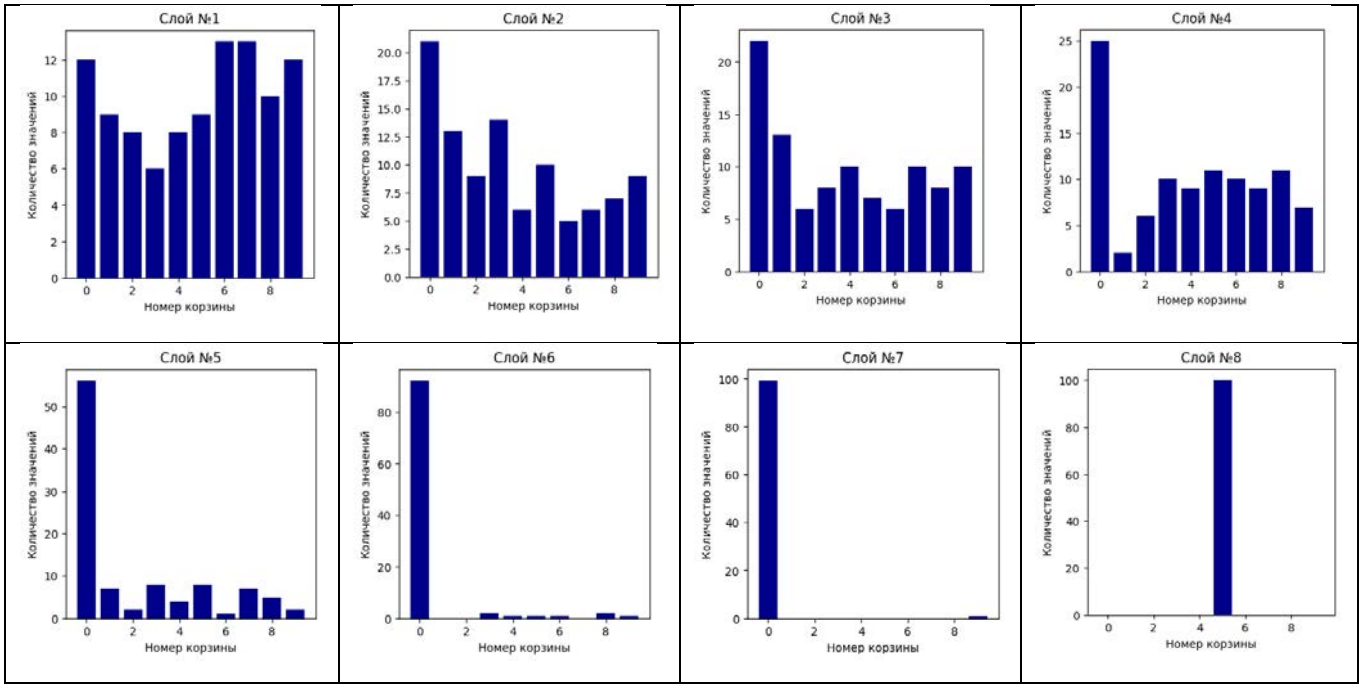


Рисунок 4.3 – Распределения значений результатов девятого NIST теста слоев первого ПО

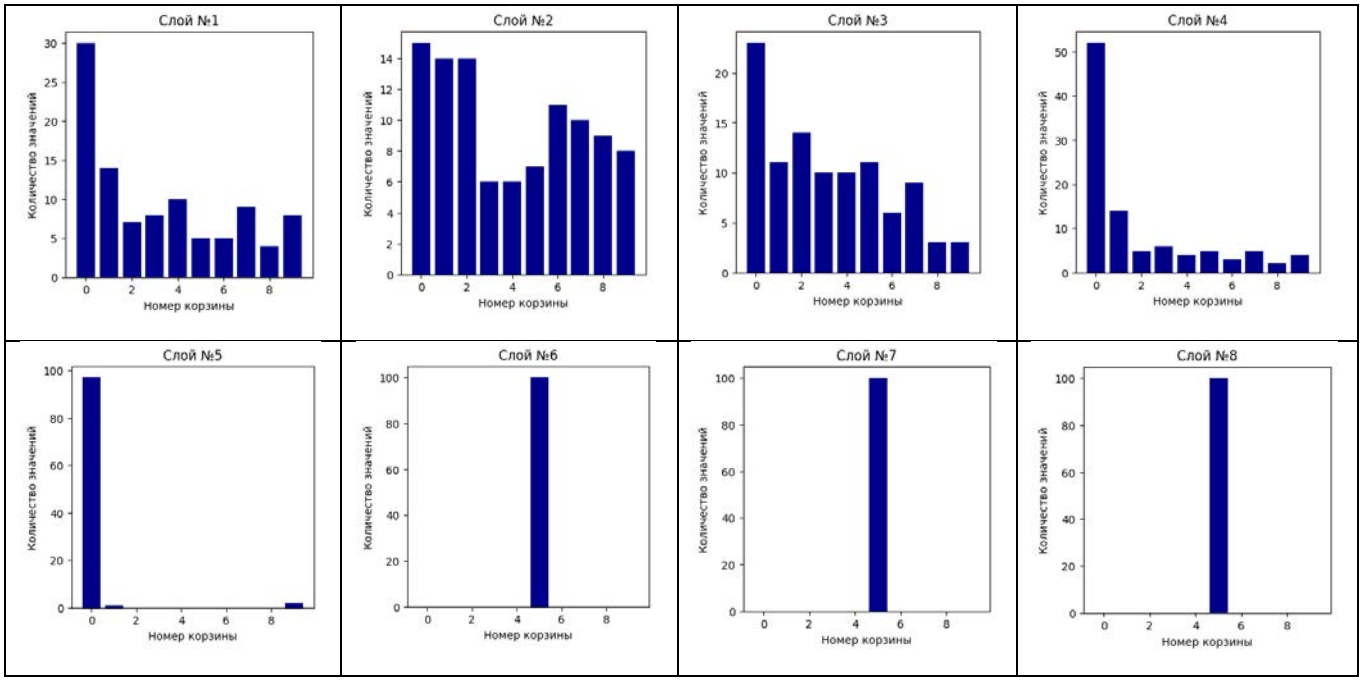


Рисунок 4.4 – Распределения значений результатов двенадцатого NIST теста слоев первого ПО

Проведем тестирование тестом №13. На рисунках 4.5 и 4.6 приведены, соответственно, результаты тестирования для первого и второго выходов 13 теста.

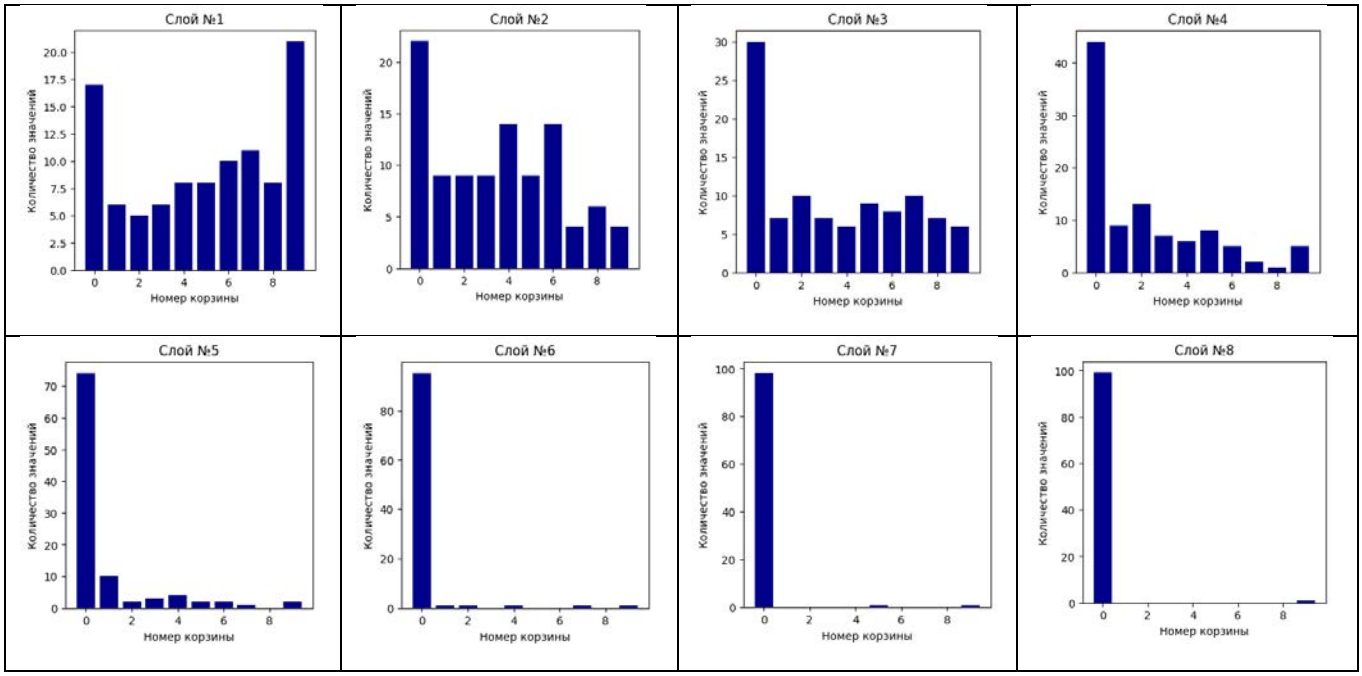


Рисунок 4.5 – Распределения значений результатов первого выхода тринадцатого NIST теста слоев первого ПО

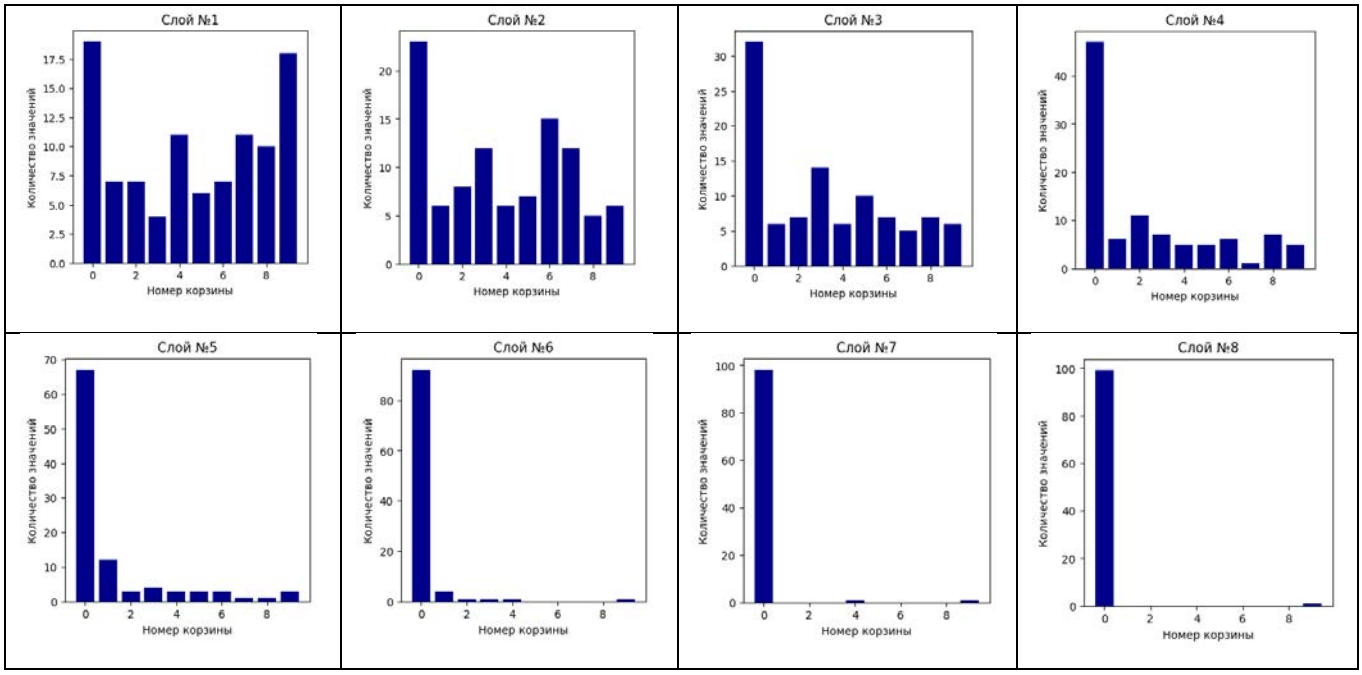


Рисунок 4.6 – Распределения значений результатов второго выхода тринадцатого NIST теста слоев первого ПО

По результатам, полученным при проведении выбранных тестов, можно увидеть, до некоторого слоя (в зависимости от теста) значения распределяются по всем корзинам. Например, на рисунке 4.4, где приведен результат теста на приблизительную энтропию, до третьего слоя включительно значения распределяются по всем корзинам с некоторым перекосам в сторону первой. Однако с четвертого уровня уже более 50% значений приходится на первую корзину. Начиная с 6-го уровня все результаты приходятся на первую корзину, что говорит о наличии закономерностей в данных. Очевидно, что для большей маскировки лучше выбирать значения из первых 3 слоев. Выбирать значения из слоев 5 и выше не рекомендуется в виду их высокой коррелированности. Проведем проверку выбранными тестами разных фрагментов. Результаты сведены в таблицу 4.1, где для каждого значения указан верхний порог рекомендуемых слоев для выбора первой компоненты, а в скобочках указан слой, выше которого результаты всех тестов попадают в первую корзину. Здесь надо понимать, что выбранные критерии достаточно условны, так как это результат анализа различных блоков данных. Тем не менее, минимальное значение в

скобках равно пяти, и оно встречается только один раз. В большинстве тестов значение 5 является приемлемым.

Таблица 4.1. – Результаты проверки разных фрагментов выбранными тестами

	Музыкальный фрагмент 1	Музыкальный фрагмент 2	Музыкальный фрагмент 3	Музыкальный фрагмент 4
Тест 1	4 (7)	5 (8)	6 (9)	5 (9)
Тест 2	5 (7)	8 (10)	7 (10)	8 (10)
Тест 9	4 (7)	8 (10)	8 (10)	8 (11)
Тест 12	3 (5)	6 (9)	6 (9)	6 (9)
Тест 13.1	4 (9)	6 (11)	5 (11)	5 (11)
Тест 13.2	4 (9)	6 (11)	5 (11)	5 (11)

Таким образом определим максимальный битовый слой для выбора первой компоненты равным 5. Заметим, что фактически речь идет о диапазоне от 2-го битового слоя до 5-го так, что большая часть выбираемых бит не будет принадлежать 5-му битовому слою.

По таблице 4.1 видно, что наиболее эффективными в плане обнаружения случайных последовательностей являются тесты 1 и 12. Таким образом, в дальнейшем будем приводить только результаты этих тестов. Тем не менее, результаты других тестов так же будут получены, но вынесены в приложения.

4.2. Исследование систем встраивания информации в пределах одного отсчета

Рассмотрим процесс встраивания двухкомпонентного контейнера в ПО используя логическую функцию связи компонент. В работах [9-11,27-34] рассматривалось встраивание на основе функции исключающее ИЛИ, так как она обладает криптографическими свойствами с одной стороны, и хорошими маскирующими свойствами с другой. Так как речь идет о блочной обработке информации, определим размер блоков для анализа. С одной стороны в системах

реального времени блоки достаточно малы (до 1024 отсчетов), с другой стороны, для статистических тестов требуются блоки большей длины (до 1 млн отсчетов). При этом криптографические алгоритмы работают с блоками 128 бит. Таким образом, встраивание будем проводить в блоки малого размера, а статистический анализ проводить по группе блоков.

4.2.1 Встраивание двух компонент в пределах одного отсчета с использованием функции исключающего ИЛИ

Проведем моделирование алгоритма, при котором две компоненты определяются в пределах одного отсчета. При этом первая компонента находится в пределах слоев 2-5, а вторая встраивается в младший битовый слой [9-11,27-34]. Стоит заметить, что данный алгоритм является потоковым.

В третьей главе мы уже формировали модель сообщения. Воспользуемся полученной моделью для формирования двухкомпонентного контейнера. Математическое описание алгоритма получено в главе 2. Учитывая, что используется только заданный диапазон выбора битовых слоев, модель (2.3) преобразуется к следующему виду:

$$\begin{cases} z_{1n} = f_1\left(k_{xnj}\right),\ j \in 2\ldots5 \\ z_{2n} = u_n \oplus z_{1n} \\ k_{yn\,i} = k_{xn\,i},\ i \in 2\ldots N \\ k_{yn\,1} = z_{2n} \end{cases} \tag{4.1}$$

Реализуем модель на языке Python. Реализация алгоритма встраивания (4.1) формируется отдельной функцией:

```
def Stego_transform(X,u,key,l):
    Y=X.copy()
    for i in range(l):
        z1=X[i,key[i]]
        z2=z1^u[i]
        Y[i,14]=z2
    return Y
```

Где X – массив отсчетов, представленных в виде битов; u – массив битов сообщения; key – массив битов ключа, определяющий расположение первой компоненты; l – количество встраиваемых бит; Y – стегосистема с встроенной скрытой информацией.

Проанализируем результат встраивания первым тестом.

Первый музыкальный фрагмент.

На рисунке 4.7 представлены гистограммы распределения значений результатов теста младшего битового слоя, который замещается встраиваемой информацией и сообщения. Проанализируем, какое воздействие на распределения окажет использование двухкомпонентного контейнера.

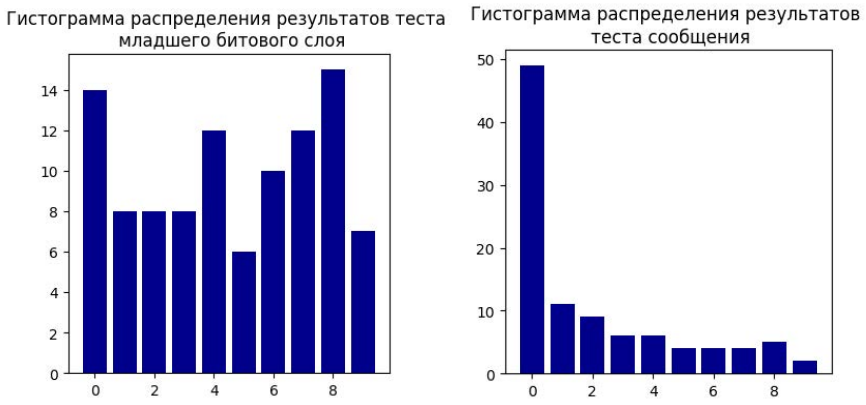


Рисунок 4.7 – Распределения значений результатов тестирования младшего битового слоя первого музыкального фрагмента и сообщения

На рисунке 4.8 представлены гистограммы распределения результатов первого теста стегосистем, сформированных на основе первого музыкального фрагмента. Выбор битового слоя первой компоненты определялся встроенным в Python генератором случайных чисел. На рисунке приведены три гистограммы. На первой гистограмме приведено распределение значений второй компоненты без предварительного криптографического шифрования. На второй гистограмме приведено распределение значений второй компоненты с предварительным шифрованием AES. Отсчеты с кружками показывают распределение результатов теста шифрованного сообщения. На третьей гистограмме приведено распределение значений второй компоненты с предварительным шифрованием

Кузнечиком. Отсчеты с кружками показывают распределение результатов теста шифрованного сообщения.

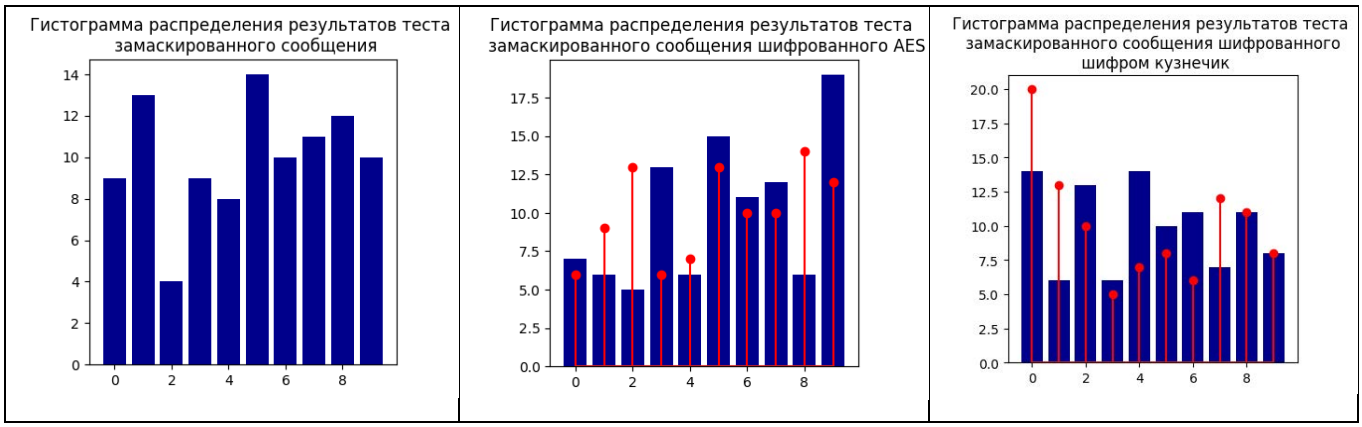


Рисунок 4.8 – Распределения значений результатов тестирования стегосистем первого музыкального фрагмента первым тестом

Второй музыкальный фрагмент.

На рисунке 4.9 представлены гистограммы распределения значений результатов теста младшего битового слоя, который замещается встраиваемой информацией. Проанализируем, какое воздействие на распределения окажет использование двухкомпонентного контейнера. На рисунке 4.10 представлены гистограммы распределения результатов первого теста стегосистем, сформированных на основе второго музыкального фрагмента. На рисунке приведены три гистограммы. На первой гистограмме приведено распределение значений второй компоненты без предварительного криптографического шифрования. На второй гистограмме приведено распределение значений второй компоненты с предварительным шифрованием AES. Отсчеты с кружками показывают распределение результатов теста шифрованного сообщения. На третьей гистограмме приведено распределение значений второй компоненты с предварительным шифрованием Кузнечиком. Отсчеты с кружками показывают распределение результатов теста шифрованного сообщения.



Рисунок 4.9 – Распределения значений результатов тестирования младшего битового слоя второго музыкального фрагмента

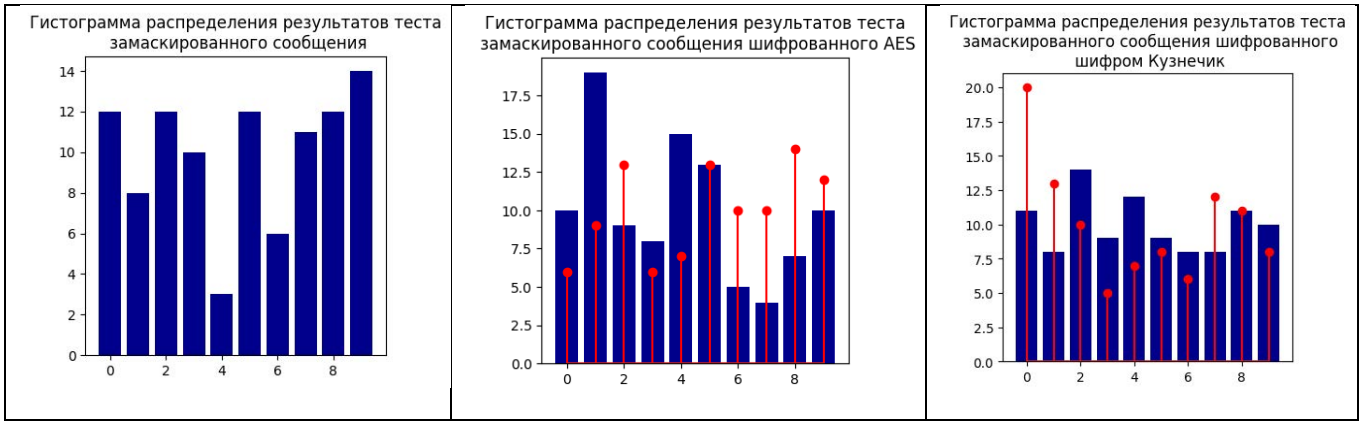


Рисунок 4.10 – Распределения значений результатов тестирования стегосистем второго музыкального фрагмента первым тестом

Третий музыкальный фрагмент.

На рисунке 4.11 представлены гистограммы распределения значений результатов теста младшего битового слоя, который замещается встраиваемой информацией. Проанализируем, какое воздействие на распределения окажет использование двухкомпонентного контейнера.



Рисунок 4.11 – Распределения значений результатов тестирования младшего битового слоя третьего музыкального фрагмента

На рисунке 4.12 представлены гистограммы распределения результатов первого теста стегосистем, сформированных на основе третьего музыкального фрагмента.

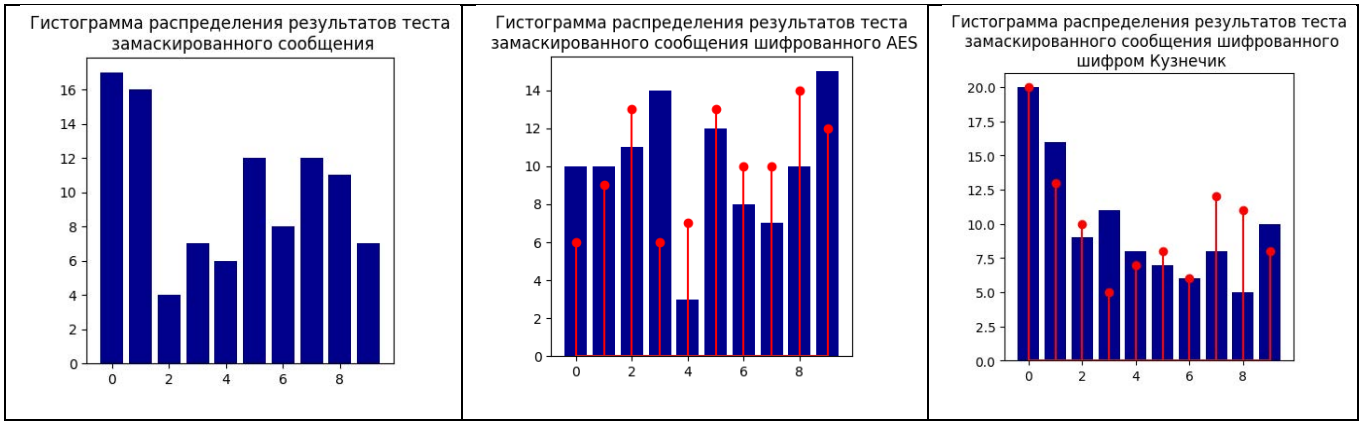


Рисунок 4.12 – Распределения значений результатов тестирования стегосистем третьего музыкального фрагмента первым тестом

На рисунке приведены три гистограммы. На первой гистограмме приведено распределение значений второй компоненты без предварительного криптографического шифрования. На второй гистограмме приведено распределение значений второй компоненты с предварительным шифрованием AES. Отсчеты с кружками показывают распределение результатов теста шифрованного сообщения. На третьей гистограмме приведено распределение значений второй компоненты с предварительным шифрованием Кузнечиком.

Отсчеты с кружками показывают распределение результатов теста шифрованного сообщения.

Четвертый музыкальный фрагмент.

На рисунке 4.13 представлены гистограммы распределения значений результатов теста младшего битового слоя, который замещается встраиваемой информацией. Проанализируем, какое воздействие на распределения окажет использование двухкомпонентного контейнера.

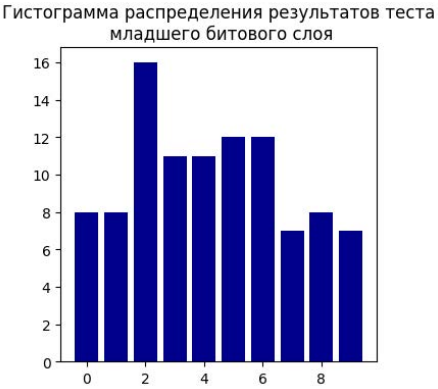


Рисунок 4.13 – Распределения значений результатов тестирования младшего битового слоя четвертого музыкального фрагмента

На рисунке 4.14 представлены гистограммы распределения результатов первого теста стегосистем, сформированных на основе четвертого музыкального фрагмента. На рисунке приведены три гистограммы. На первой гистограмме приведено распределение значений второй компоненты без предварительного криптографического шифрования. На второй гистограмме приведено распределение значений второй компоненты с предварительным шифрованием AES. Отсчеты с кружками показывают распределение результатов теста шифрованного сообщения. На третьей гистограмме приведено распределение значений второй компоненты с предварительным шифрованием Кузнечиком. Отсчеты с кружками показывают распределение результатов теста шифрованного сообщения.

По гистограммам, полученным в результате проведения первого теста можно сделать вывод, что при использовании незашифрованного сообщения,

совместно с двухкомпонентным контейнером наблюдается значительное улучшение статистических характеристик. Использование двухкомпонентного контейнера совместно с шифром AES не дает ярко выраженного результата. Использование двухкомпонентного контейнера совместно с шифром Кузнечик в некоторой степени сглаживает гистограмму.

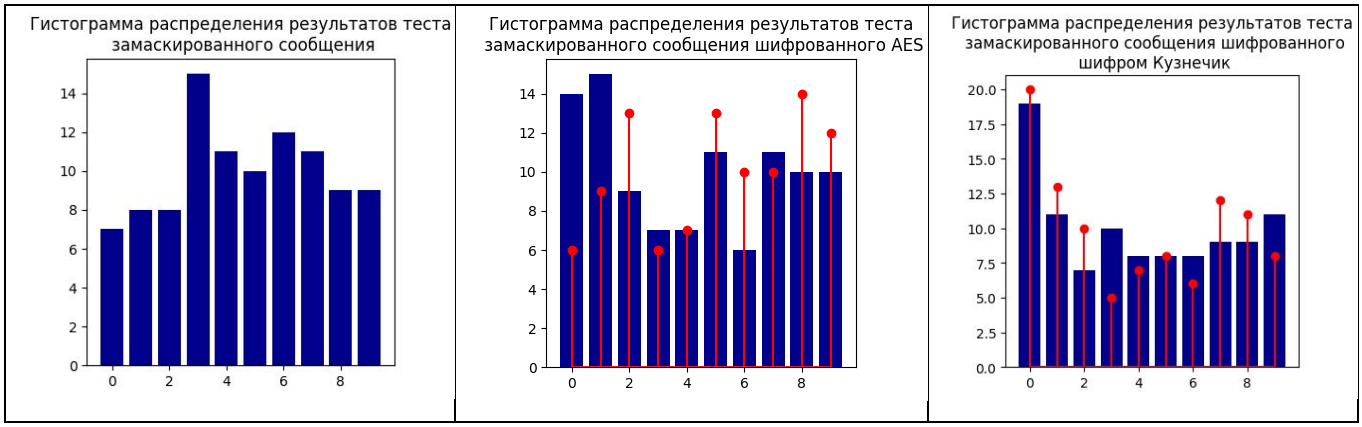


Рисунок 4.14 – Распределения значений результатов тестирования стегосистем четвертого музыкального фрагмента первым тестом

Проведем тестирование двенадцатым тестом.

Первый музыкальный фрагмент.

На рисунке 4.15 представлены гистограммы распределения значений результатов теста младшего битового слоя, который замещается встраиваемой информацией и сообщения. Проанализируем, какое воздействие на распределения окажет использование двухкомпонентного контейнера.

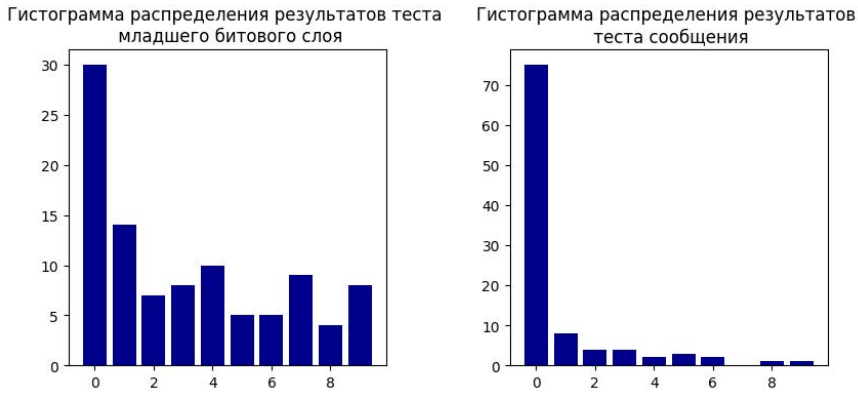


Рисунок 4.15 – Распределения значений результатов тестирования младшего битового слоя первого музыкального фрагмента и сообщения

На рисунке 4.16 представлены гистограммы распределения результатов двенадцатого теста стегосистем, сформированных на основе первого музыкального фрагмента.

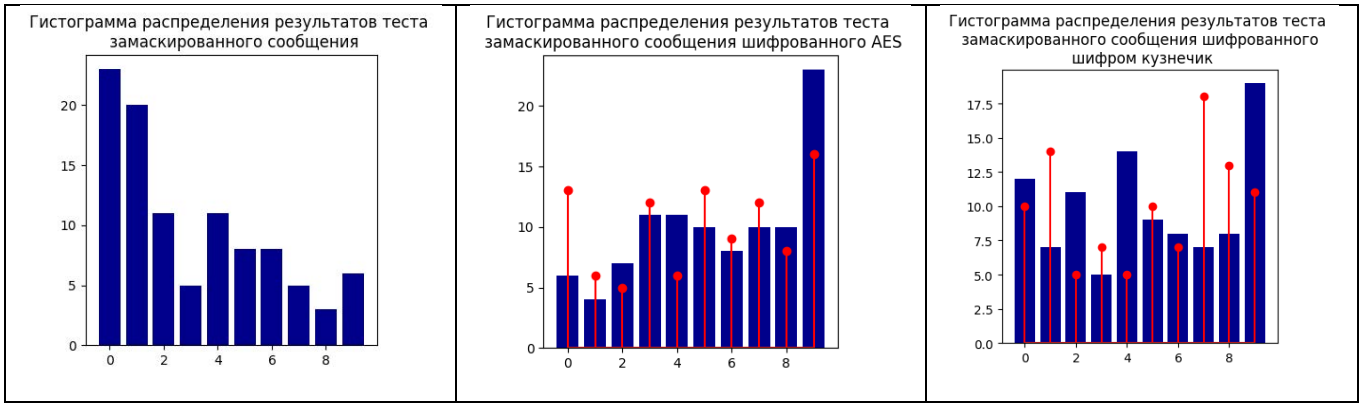


Рисунок 4.16 – Распределения значений результатов тестирования стегосистем первого музыкального фрагмента двенадцатым тестом

На рисунке приведены три гистограммы. На первой гистограмме приведено распределение значений второй компоненты без предварительного криптографического шифрования. На второй гистограмме приведено распределение значений второй компоненты с предварительным шифрованием AES. Отсчеты с кружками показывают распределение результатов теста шифрованного сообщения. На третьей гистограмме приведено распределение значений второй компоненты с предварительным шифрованием Кузнечиком. Отсчеты с кружками показывают распределение результатов теста шифрованного сообщения.

Второй музыкальный фрагмент.

На рисунке 4.17 представлены гистограммы распределения значений результатов теста младшего битового слоя, который замещается встраиваемой информацией. Проанализируем, какое воздействие на распределения окажет использование двухкомпонентного контейнера. На рисунке 4.18 представлены гистограммы распределения результатов двенадцатого теста стегосистем, сформированных на основе второго музыкального фрагмента. На рисунке приведены три гистограммы. На первой гистограмме приведено распределение значений второй компоненты без предварительного криптографического

шифрования. На второй гистограмме приведено распределение значений второй компоненты с предварительным шифрованием AES. Отсчеты с кружками показывают распределение результатов теста шифрованного сообщения. На третьей гистограмме приведено распределение значений второй компоненты с предварительным шифрованием Кузнечиком. Отсчеты с кружками показывают распределение результатов теста шифрованного сообщения.



Рисунок 4.17 – Распределения значений результатов тестирования младшего битового слоя второго музыкального фрагмента

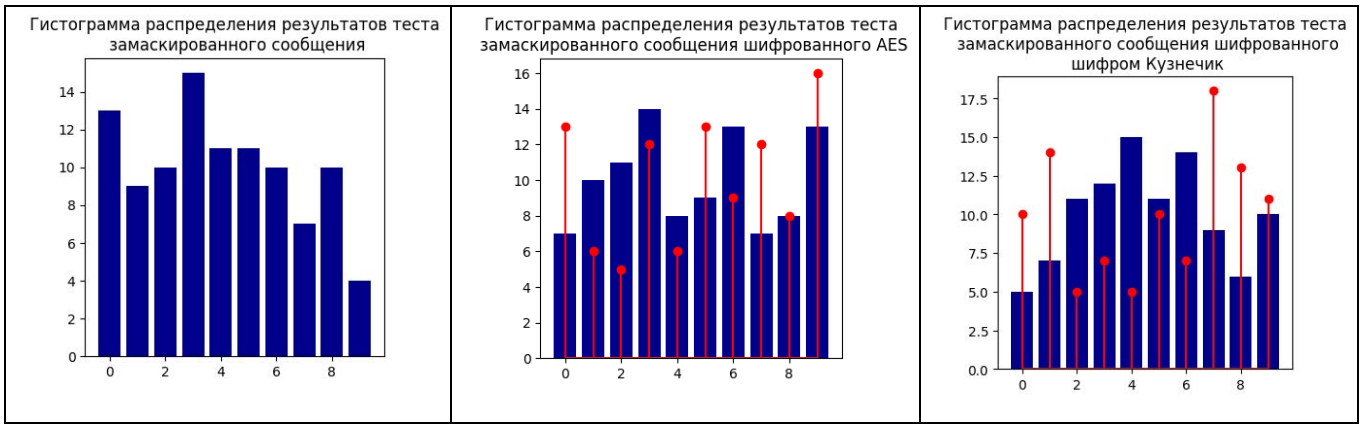


Рисунок 4.18 – Распределения значений результатов тестирования стегосистем второго музыкального фрагмента двенадцатым тестом

Третий музыкальный фрагмент.

На рисунке 4.19 представлены гистограммы распределения значений результатов теста младшего битового слоя, который замещается встраиваемой информацией. Проанализируем, какое воздействие на распределения окажет использование двухкомпонентного контейнера.



Рисунок 4.19 – Распределения значений результатов тестирования младшего битового слоя третьего музыкального фрагмента

На рисунке 4.20 представлены гистограммы распределения результатов двенадцатого теста стегосистем, сформированных на основе третьего музыкального фрагмента. На рисунке приведены три гистограммы. На первой гистограмме приведено распределение значений второй компоненты без предварительного криптографического шифрования. На второй гистограмме приведено распределение значений второй компоненты с предварительным шифрованием AES. Отсчеты с кружками показывают распределение результатов теста шифрованного сообщения. На третьей гистограмме приведено распределение значений второй компоненты с предварительным шифрованием Кузнечиком. Отсчеты с кружками показывают распределение результатов теста шифрованного сообщения.



Рисунок 4.20 – Распределения значений результатов тестирования стегосистем третьего музыкального фрагмента двенадцатым тестом

Четвертый музыкальный фрагмент.

На рисунке 4.21 представлены гистограммы распределения значений результатов теста младшего битового слоя, который замещается встраиваемой информацией. Проанализируем, какое воздействие на распределения окажет использование двухкомпонентного контейнера.

На рисунке 4.22 представлены гистограммы распределения результатов двенадцатого теста стегосистем, сформированных на основе четвертого музыкального фрагмента. На рисунке приведены три гистограммы. На первой гистограмме приведено распределение значений второй компоненты без предварительного криптографического шифрования. На второй гистограмме приведено распределение значений второй компоненты с предварительным шифрованием AES. Отсчеты с кружками показывают распределение результатов теста шифрованного сообщения. На третьей гистограмме приведено распределение значений второй компоненты с предварительным шифрованием Кузнечиком. Отсчеты с кружками показывают распределение результатов теста шифрованного сообщения.



Рисунок 4.21 – Распределения значений результатов тестирования младшего битового слоя четвертого музыкального фрагмента

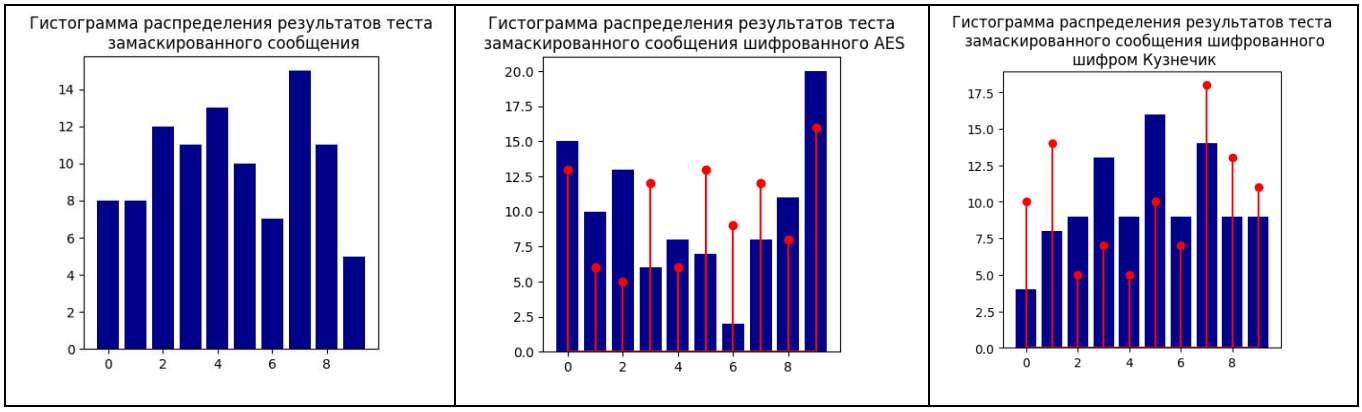


Рисунок 4.22 – Распределения значений результатов тестирования стегосистем четвертого музыкального фрагмента двенадцатым тестом

По гистограммам, полученным в результате проведения второго теста можно сделать вывод, что наилучшее распределение наблюдается при использовании комбинации двухкомпонентного контейнера совместно с шифром AES.

Результаты тестирования вторым, девятым и тринадцатыми тестами приведены в приложении 3.1.

По проделанным экспериментам можно сделать вывод, что использование незашифрованных данных крайне не рекомендуется, так как статистически легко определяется. Использование блочных шифров (AES, Кузнечик) преобразует поток битов к виду, имеющему статистические характеристики случайной последовательности, что наряду с использованием двухкомпонентного контейнера позволяет эффективно маскировать информацию в младшем битовом слое, так как в несжатых ПО младший битовый слой зачастую имеет именно характер случайной последовательности. Как было показано в главе – чем старше битовый слой – тем реже он проходит тест на случайность, что ограничивает встраивание информации в зашифрованном виде, так как может быть легко обнаружено статистически.

4.2.2 Многослойное встраивание двух компонент в пределах одного отсчета с использованием функции исключающего ИЛИ

Рассмотрим многослойное встраивание сообщения в пределах одного отсчета. Как было указано в главе 2, в соответствии с математической моделью (2.4), встраивание выполняется итерационно. Встроим четыре слоя сообщения в звуковые фрагменты и оценим воздействие двухкомпонентного контейнера на статистические свойства стегосистемы. С учетом модели 4.1 и 4 слоев встраивания модель 2.4 преобразуется к виду:

$$\begin{cases} z_{1n}^{l} = f_1\left(k_{xnj1}^{l}\right), \ \ j \in 2+l \ldots 5+l \\ z_{2n}^{l} = u_n^{l} \oplus z_{1n}^{l} \\ k_{x-1\,n\,i}^{l} = k_{x\,n\,i}^{l}, i \in 2 \ldots N \\ k_{x-1\,n\,1}^{l} = z_{2n}^{l} \end{cases} \tag{4.2}$$

Проведем моделирование. Основная часть результатов моделирования помещена в приложение 3.2. Рассмотрим основные моменты. Очевидно, что чем выше битовый слой, тем менее вероятно он будет шумоподобным, что объясняется осмысленностью информации звукового ПО. На рисунке 4.23 можно увидеть изменение результатов первого теста битовых слоев первого музыкального фрагмента, в зависимости от уровня слоя (для четырех младших слоев). Результат тестирования второго музыкального фрагмента приведен на рисунке 4.24.

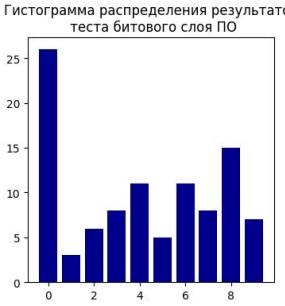
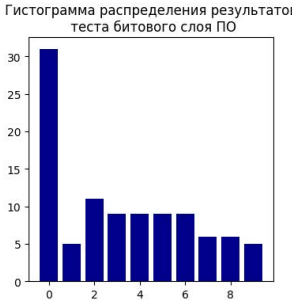
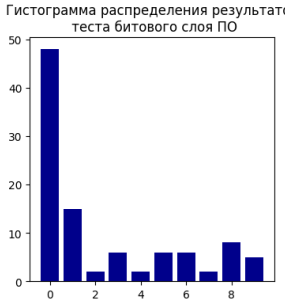
Младший нулевой битовый слой	Первый битовый слой	Второй битовый слой	Третий битовый слой
			

Рисунок 4.23 – Распределения значений результатов тестирования битовых слоев первого музыкального фрагмента первым тестом

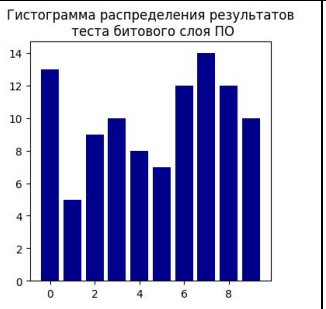
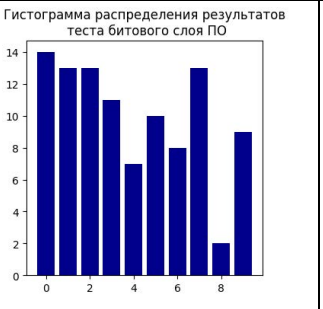
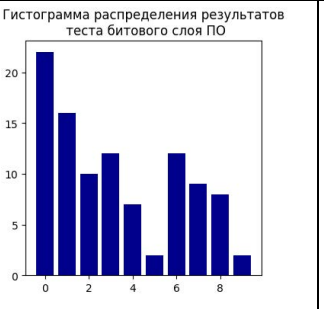
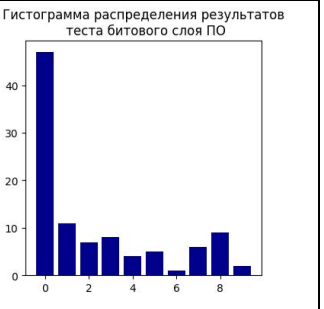
Младший нулевой битовый слой	Первый битовый слой	Второй битовый слой	Третий битовый слой
			

Рисунок 4.24 – Распределения значений результатов тестирования битовых слоев второго музыкального фрагмента первым тестом

Остальные фрагменты имеют схожие результаты, то есть, чем старше слой, тем менее случайный характер имеют битовые слои. При этом использование криптографического шифрования приводит к тому, что зашифрованная последовательность имеет случайный характер. Рассмотрим, как влияет использование многослойного встраивания двухкомпонентного контейнера на четыре младших битовых слоя.

На рисунке 4.25 приведен результат исследования встраивания с помощью двухкомпонентного метода незашифрованного сообщения.

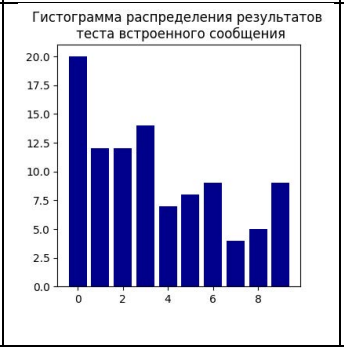
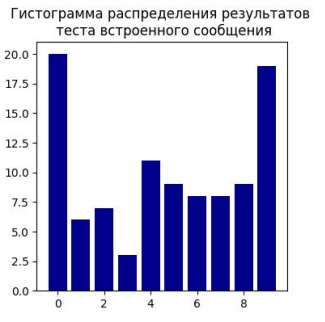
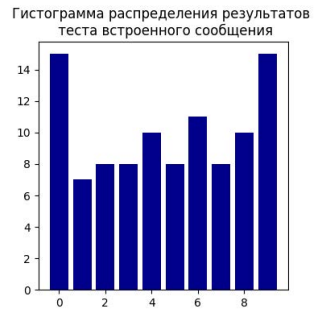
Младший нулевой битовый слой	Первый битовый слой	Второй битовый слой	Третий битовый слой
			

Рисунок 4.25 – Распределения значений результатов тестирования битовых слоев стегосистемы первым тестом

На рисунке 4.26 приведен результат встраивания сообщения, зашифрованного шифром AES. Отсчеты с кружками показывают распределение значений зашифрованного сообщения.

На рисунке 4.27 приведен результат встраивания сообщения, зашифрованного шифром Кузнечик. Отсчеты с кружками показывают распределение значений зашифрованного сообщения.

Видно, что в данном случае влияние старших слоев при встраивании не оказывает решающего воздействия на распределения, несмотря на использование старших слоев в качестве источника первой компоненты. Таким образом можно заключить, что использование многослойного встраивания имеет свои ограничения и может быть обнаружено при задействовании нескольких слоев ПО для встраивания.

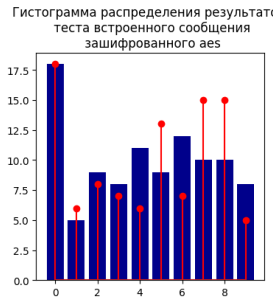
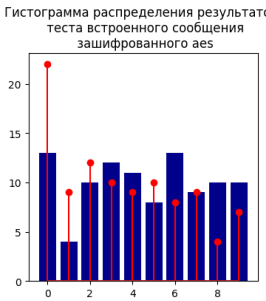
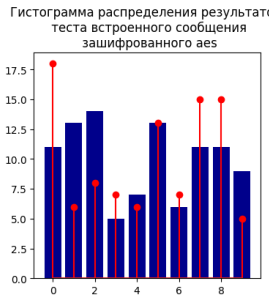
Младший нулевой битовый слой	Первый битовый слой	Второй битовый слой	Третий битовый слой
			

Рисунок 4.26 – Распределения значений результатов тестирования битовых слоев стегосистемы первым тестом

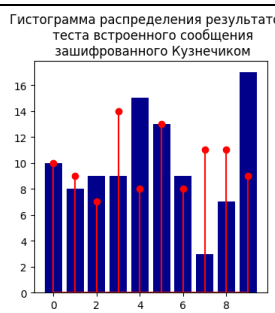
Младший нулевой битовый слой	Первый битовый слой	Второй битовый слой	Третий битовый слой
			

Рисунок 4.27 – Распределения значений результатов тестирования битовых слоев стегосистемы первым тестом

Проведем эксперимент с использованием двенадцатого теста. На рисунке 4.28 приведен анализ изменения результатов двенадцатого теста битовых слоев

первого музыкального фрагмента, в зависимости от уровня слоя (для четырех младших слоев). На рисунке 4.29 приведен результат тестирования стегосистемы с использованием незашифрованного сообщения.

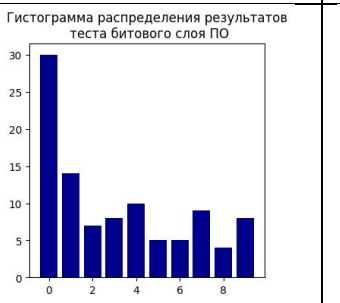
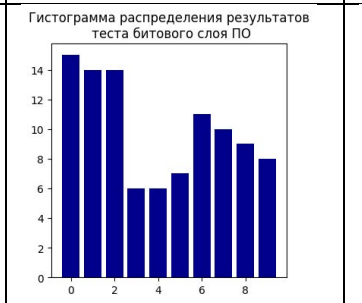
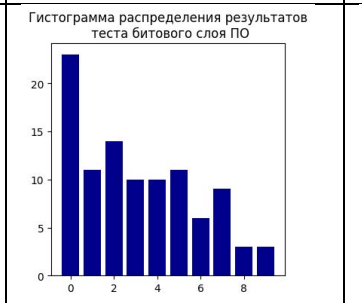
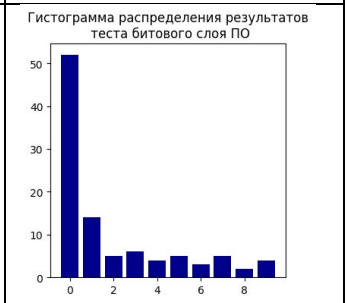
Младший нулевой битовый слой	Первый битовый слой	Второй битовый слой	Третий битовый слой
			

Рисунок 4.28 – Распределения значений результатов тестирования битовых слоев ПО двенадцатым тестом

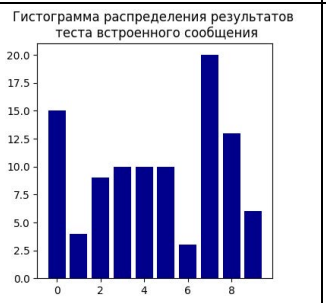
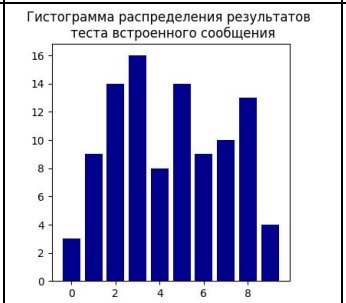
Младший нулевой битовый слой	Первый битовый слой	Второй битовый слой	Третий битовый слой
			

Рисунок 4.29 – Распределения значений результатов тестирования битовых слоев стегосистемы первым тестом

На рисунке 4.30 приведен результат встраивания сообщения, зашифрованного шифром AES. Отсчеты с кружками показывают распределение значений зашифрованного сообщения.

На рисунке 4.31 приведен результат встраивания сообщения, зашифрованного шифром Кузнечик. Отсчеты с кружками показывают распределение значений зашифрованного сообщения.

Видно, что результаты, полученные с помощью двенадцатого теста, не противоречат приведенному выше утверждению. Таким образом, встраивание в

пределах отсчета с использованием многослойного контейнера в более чем два слоя статистически может быть обнаружено.

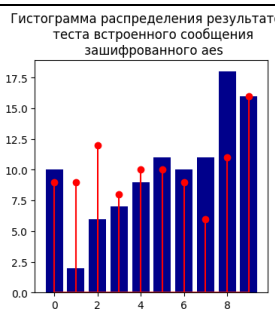
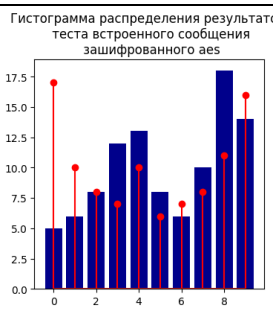
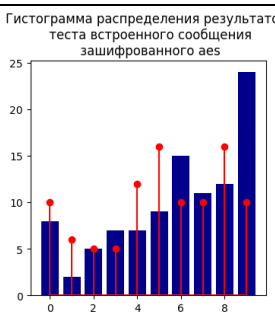
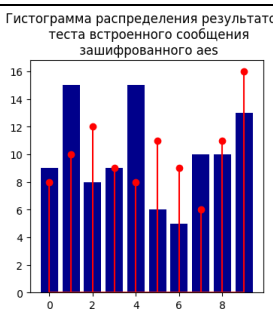
Младший нулевой битовый слой	Первый битовый слой	Второй битовый слой	Третий битовый слой
			

Рисунок 4.30 – Распределения значений результатов тестирования битовых слоев стегосистемы первым тестом

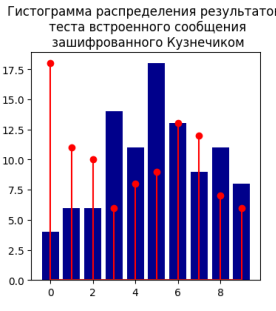
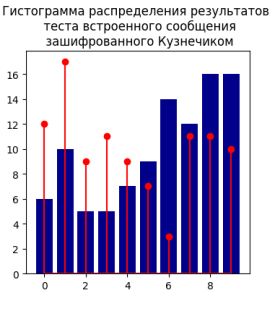
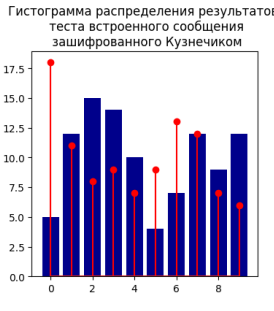
Младший нулевой битовый слой	Первый битовый слой	Второй битовый слой	Третий битовый слой
			

Рисунок 4.31 – Распределения значений результатов тестирования битовых слоев стегосистемы первым тестом

Встраивание информации в пределах одного отсчета осложняет адаптацию системы. Рассмотрим встраивание с помощью двухкомпонентного контейнера при оконной обработке информации.

4.3. Исследование систем встраивания информации в пределах окна фиксированного размера

Рассмотрим процесс оконного встраивания двухкомпонентного контейнера в ПО используя логические функции связи компонент. В работах [36,37]

рассматривалось встраивание двухкомпонентного контейнера в пределах окна фиксированного размера. Очевидно, что в данном случае источником первой компоненты может выступать не только отсчет, куда выполняется встраивание, но весь массив бит старших слоев окна ПО. Это позволяет не только отвязаться от отсчета, но и внести элемент адаптации алгоритма к старшим слоям ПО. В работе [37] показано, что переход от одного отсчета к окну, фактически, не меняет степень маскировки. Проведем моделирование различных режимов встраивания информации в пределах окна.

4.3.1 Модель стеганографической системы использующей встраивание двух компонент в пределах окна фиксированного размера с использованием функции исключающего ИЛИ

Проведем моделирование алгоритма, описанного математической моделью (2.8) и сравним результаты с полученными в предыдущем параграфе. В модели использовано окно размером 128 отсчетов. Проведем встраивание информации в первый музыкальный фрагмент. На рисунке 4.7 приведен результат анализа ПО и сообщения первым тестом. На рисунке 4.32 представлены гистограммы распределения результатов первого теста стегосистем, сформированных на основе первого музыкального фрагмента. Выбор битового слоя первой компоненты, как и в предыдущих моделях, определялся встроенным в Python генератором случайных чисел. На рисунке 4.32 приведены три гистограммы. На первой гистограмме приведено распределение значений второй компоненты без предварительного криптографического шифрования. На второй гистограмме приведено распределение значений второй компоненты с предварительным шифрованием AES. Отсчеты с кружками показывают распределение результатов теста шифрованного сообщения. На третьей гистограмме приведено распределение значений второй компоненты с предварительным шифрованием Кузнечиком. Отсчеты с кружками показывают распределение результатов теста шифрованного сообщения.

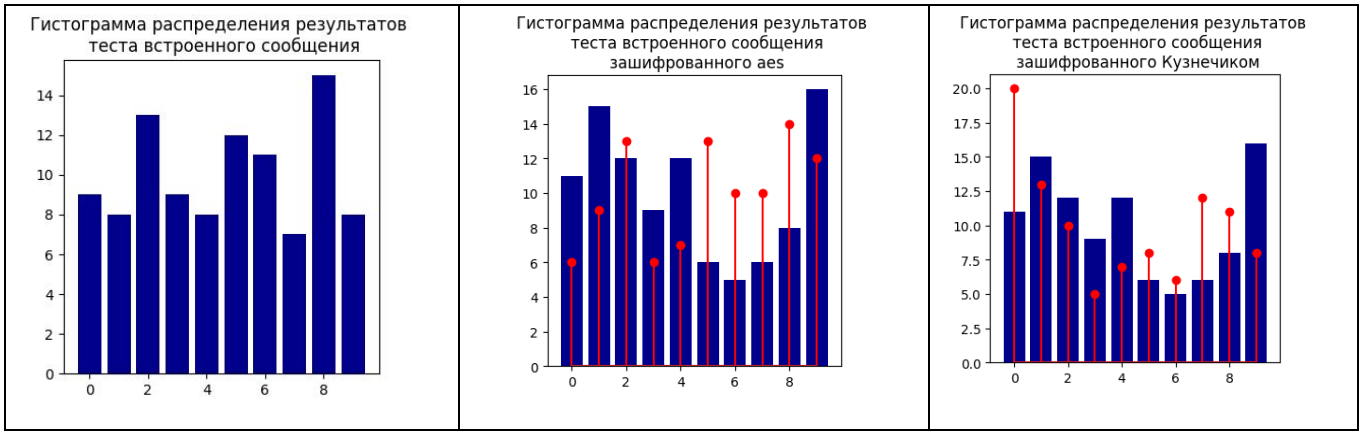


Рисунок 4.32 – Распределения значений результатов тестирования стегосистем первого музыкального фрагмента первым тестом

Предсказуемо, встраивание показывает хорошие результаты, в младшем слое ПО как при использовании шифрования, так и без него. Более того, как показано в работе [35], использование окна нивелирует появление нулевых отсчетов при их единичном проявлении. На рисунке 4.33 приведены результаты распределения значений результатов тестирования стегосистем второго музыкального фрагмента первым тестом. Гистограмма распределения результатов теста младшего битового слоя приведена на рисунке 4.9. Видно, что результаты встраивания, как и для первого фрагмента, дают хороший результат маскировки. Эксперименты, проведенные для остальных фрагментов, так же дают хороший уровень маскировки. Эксперименты с другими тестами так же подтверждают полученный результат. Проведем эксперимент с многослойным встраиванием в пределах окна.

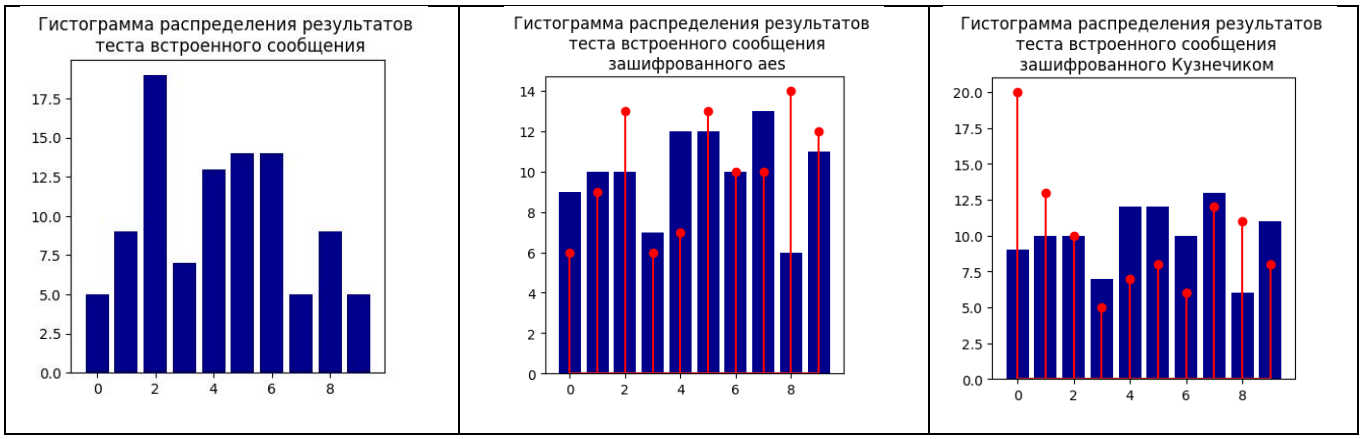


Рисунок 4.33 – Распределения значений результатов тестирования стегосистем первого музыкального фрагмента первым тестом

4.3.2 Модель стеганографической системы, использующей встраивание двух компонент в пределах окна фиксированного размера с использованием условных функций определения второй компоненты стегоконтейнера

Проведем моделирование алгоритма, описанного математической моделью (2.10). Определим количество слоев встраивания равным четырем. Данное значение выбрано исходя из характера статистических характеристик ПО, проанализированных в третьей главе.

При известном количестве отсчетов в окне M, и известном количестве слоев встраивания, равном четырем, количество бит встраивания определится, как $4M$. Столько же ключей понадобится. Как и в предыдущем параграфе ПО разбивается на окна фиксированной длины, затем выполняется встраивание. При этом, на первом этапе встраивание осуществляется в 3-й слой (нулевой слой младший), после заполнения всех бит нулевого слоя, начинается встраивание во 2-й слой и т.д. При этом в модели предусмотрен выбор ключа и четырех слоев старше того, в который осуществляется встраивание. Таким образом, уже при переходе к встраиванию во 2-й слой, в качестве ключа могут выбираться биты из 1-го слоя, заполненного встроенными значениями. Рассмотрим результат моделирования. На рисунке 4.34 представлены распределения результатов тестирования первым тестом младшего (нулевого) битового слоя ПО (первого музыкального фрагмента) и сообщения. Несмотря на то, что встраивание производилось с 3-го слоя и до нулевого, рассмотрим результаты от нулевого (младшего), до 3-го слоя.

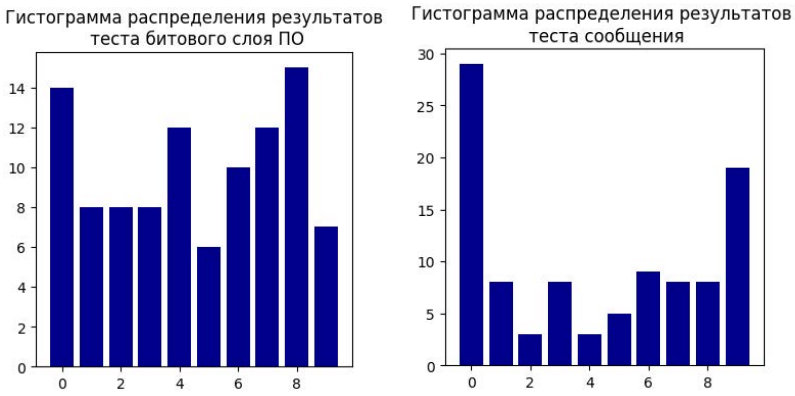


Рисунок 4.34 – Распределения значений результатов тестирования младшего битового слоя первого музыкального фрагмента и сообщения

На рисунке 4.35 представлены гистограммы распределения результатов первого теста младшего битового слоя стегосистем, сформированных на основе первого музыкального фрагмента.

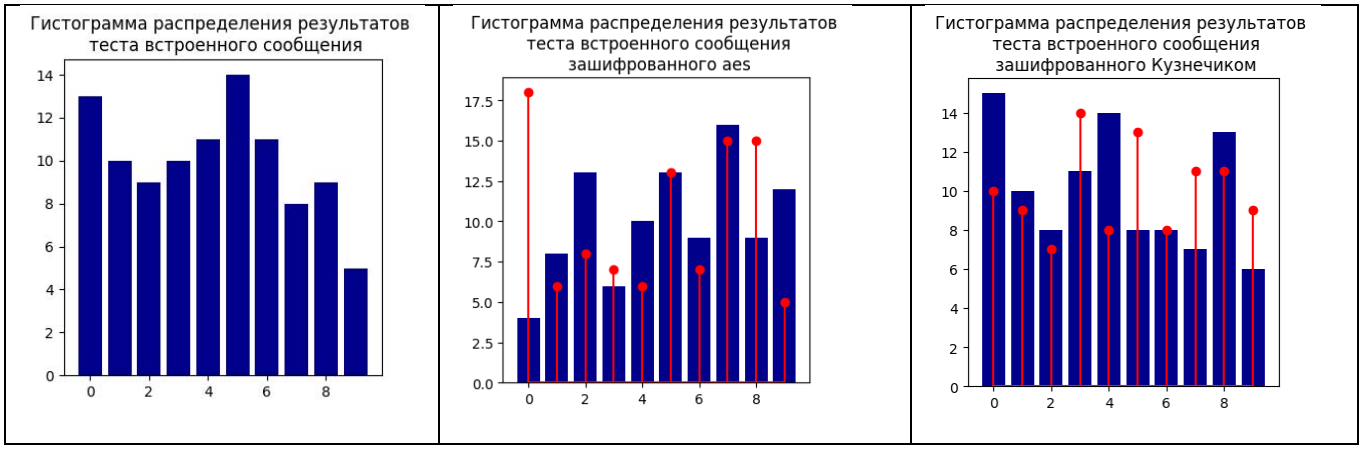


Рисунок 4.35 – Распределения значений результатов тестирования нулевого слоя стегосистем первого музыкального фрагмента первым тестом.

Как и в предыдущем параграфе видно, что встраивание в младший битовый слой эффективно маскирует сообщение. Рассмотрим встраивание в другие битовые слои. На рисунке 4.36 представлены распределения результатов тестирования первым тестом 1-го битового слоя ПО (первого музыкального фрагмента) и сообщения. Битовая последовательность сообщения, в данном случае, отличается от битовой последовательности сообщения, маскируемой в младшем битовом слое.

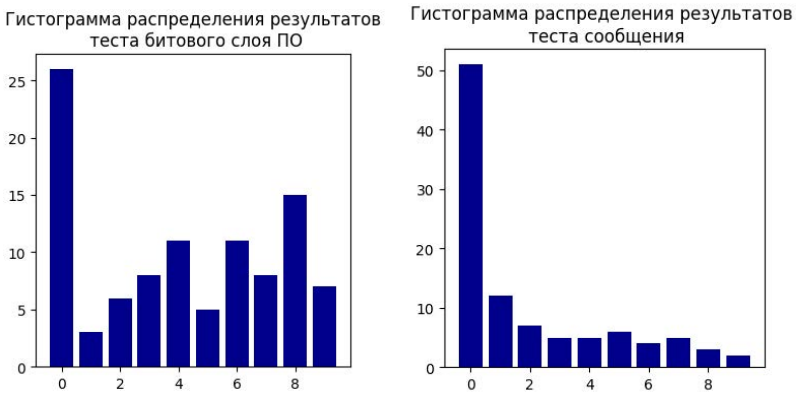


Рисунок 4.36 – Распределения значений результатов тестирования 1-го битового слоя первого музыкального фрагмента и сообщения

На рисунке 4.37 представлены гистограммы распределения результатов первого теста 1-го битового слоя стегосистем, сформированных на основе первого музыкального фрагмента.

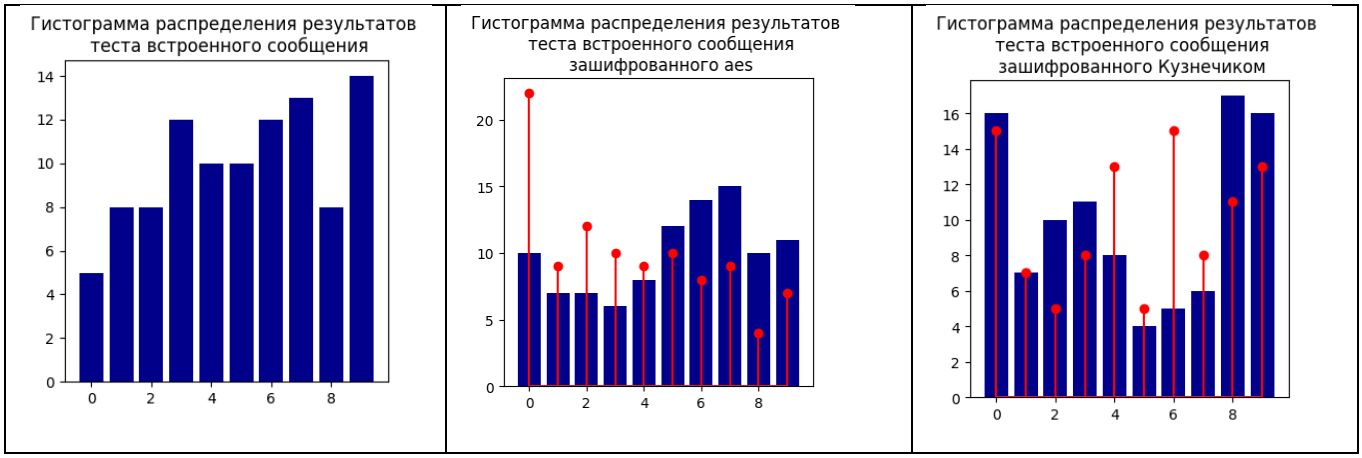


Рисунок 4.37 – Распределения значений результатов тестирования 1-го слоя стегосистем первого музыкального фрагмента первым тестом.

Рассмотрим результат встраивания во 2-й битовый слой. На рисунке 4.38 представлены распределения результатов тестирования первым тестом 2-го битового слоя покрывающего объекта (первого музыкального фрагмента) и сообщения.

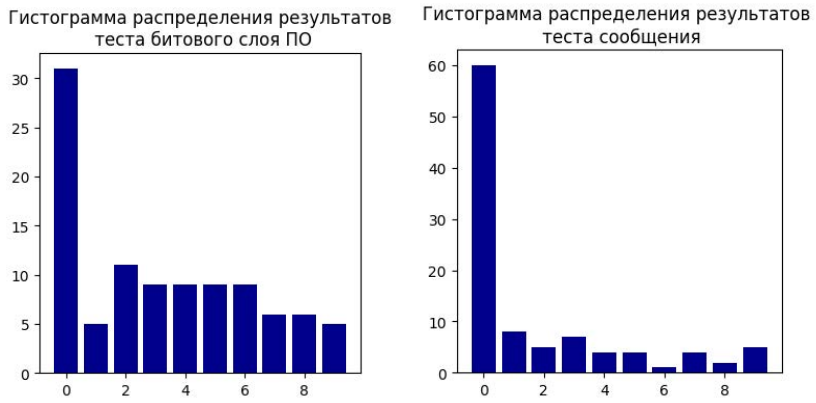


Рисунок 4.38 – Распределения значений результатов тестирования 2-го битового слоя первого музыкального фрагмента и сообщения

Можно увидеть, что статистический характер битового слоя имеет менее случайный характер, и приблизился к характеру сообщения.

На рисунке 4.39 представлены гистограммы распределения результатов первого теста 2-го битового слоя стегосистем, сформированных на основе первого музыкального фрагмента. Видно, что характер зашифрованных последовательностей не меняется. При встраивании во 2-й битовый слой эти последовательности могут быть обнаружены.

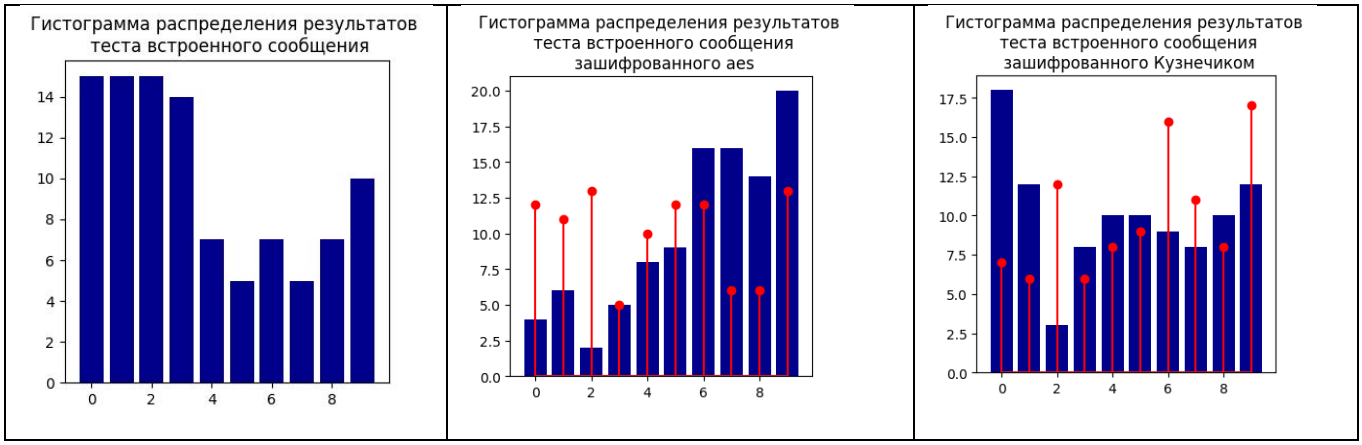


Рисунок 4.39 – Распределения значений результатов тестирования 2-го слоя стегосистем первого музыкального фрагмента первым тестом.

Рассмотрим результат встраивания в 3-й битовый слой. На рисунке 4.40 представлены распределения результатов тестирования первым тестом 3-го битового слоя ПО (первого музыкального фрагмента) и сообщения.

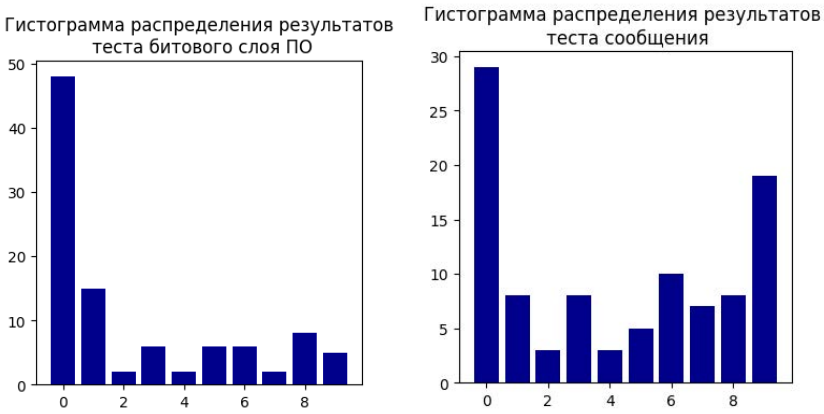


Рисунок 4.40 – Распределения значений результатов тестирования 3-го битового слоя первого музыкального фрагмента и сообщения

Можно увидеть, что статистический характер битового слоя имеет менее случайный характер, и приблизился к характеру сообщения.

На рисунке 4.41 представлены гистограммы распределения результатов первого теста 3-го битового слоя стегосистем, сформированных на основе первого музыкального фрагмента.

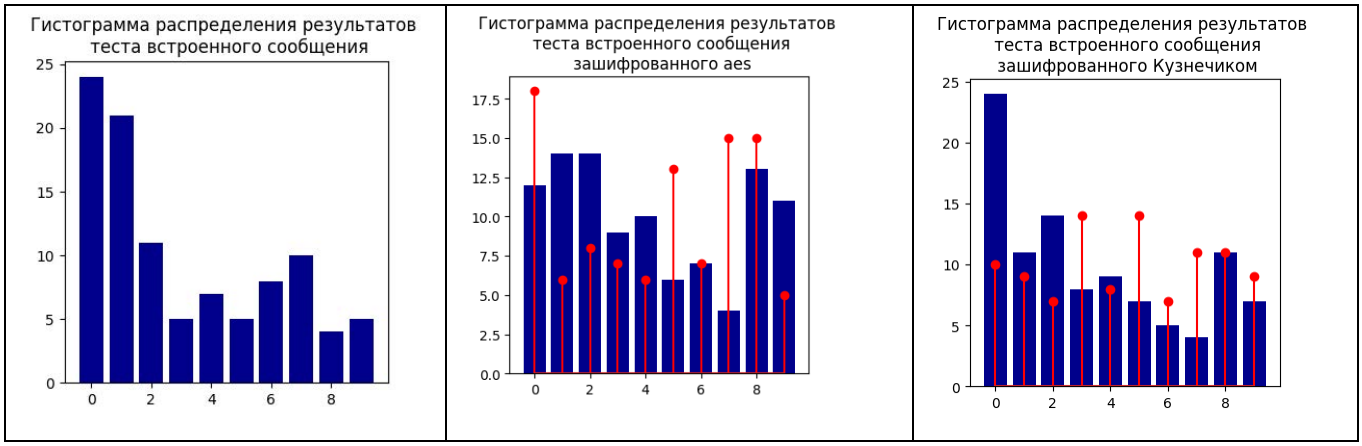


Рисунок 4.41 – Распределения значений результатов тестирования 3-го слоя стегосистем первого музыкального фрагмента первым тестом.

По приведенному выше анализу можно увидеть, что встраивание больше чем в два слоя становится статистически заметным. Сведем в таблицы результаты исследования четырех музыкальных фрагментов всеми тестами.

В таблице 4.2 сведены результаты рассмотренного выше тестирования первым тестом результатов встраивания в первый музыкальный фрагмент.

Таблица 4.2. – Результаты тестирования первым тестом встраивания информации в первый музыкальный фрагмент

	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

В таблице 4.3 сведены результаты рассмотренного выше тестирования первым тестом результатов встраивания во второй музыкальный фрагмент.

Таблица 4.3. – Результаты тестирования первым тестом встраивания информации во второй музыкальный фрагмент

	Битовый слой	Сообщение	Встраивание без шифрования	Встраивание с шифрованием AES	Встраивание с шифрованием Кузнечиком
Уровень 3	47	29	22	17	3
Уровень 2	22	60	9	18	20
Уровень 1	14	51	8	3	11
Уровень 0 (младший)	13	29	6	4	12

В таблице 4.4 сведены результаты рассмотренного выше тестирования первым тестом результатов встраивания в третий музыкальный фрагмент.

Таблица 4.4. – Результаты тестирования первым тестом встраивания информации в третий музыкальный фрагмент

	Битовый слой	Сообщение	Встраивание без шифрования	Встраивание с шифрованием AES	Встраивание с шифрованием Кузнечиком
Уровень 3	2	29	16	10	20
Уровень 2	9	60	25	10	3
Уровень 1	17	51	11	11	8
Уровень 0 (младший)	9	29	14	11	11

В таблице 4.5 сведены результаты рассмотренного выше тестирования первым тестом результатов встраивания в четвертый музыкальный фрагмент.

Таблица 4.5. – Результаты тестирования первым тестом встраивания информации в четвертый музыкальный фрагмент

	Битовый слой	Сообщение	Встраивание без шифрования	Встраивание с шифрованием AES	Встраивание с шифрованием Кузнечиком
Уровень 3	29	29	9	10	3
Уровень 2	14	60	18	15	14
Уровень 1	22	51	8	6	18
Уровень 0 (младший)	8	29	27	11	23

В таблице 4.5 сведены результаты рассмотренного выше тестирования вторым тестом результатов встраивания в первый музыкальный фрагмент.

Проведенное исследование показывает, что все выбранные тесты только подтверждают результаты, полученные первым тестом. Очевидно, что многоуровневое встраивание с помощью двухкомпонентного контейнера зашифрованных сообщений становится заметным сразу, как только меняется статистический характер слоев ПО [5]. Для примера, на рисунке 4.42 приведен график зависимости величины первого столбца гистограммы распределений результатов первого теста ПО и стегосистемы без шифрования в зависимости от уровня битового слоя. График с маркерами соответствует битовым слоям ПО.

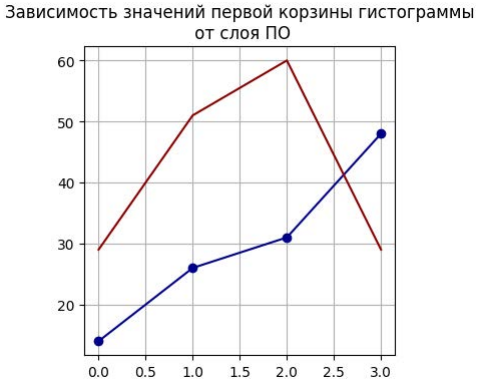


Рисунок 4.42 – Зависимость амплитуды первого столбца гистограммы распределения результатов первого теста музыкального фрагмента от битового слоя

При этом встраивание без шифрования имеет несколько лучшие результаты, однако это частный случай, определяемый характером сообщения. Для снижения

заметности предлагается использовать адаптацию к характеристикам ПО за счет варьирования логических функций встраивания, как было показано в параграфе 2.3, в частности в математической модели (2.11). Для построения модели требуется в дополнение к ключу определить количество NP точек анализа старших слоев ПО, и, для каждого встраиваемого значения (бита) сообщения определить координаты этих точек. В построенной модели координаты точек проверки определяются в диапазоне четырех старших слоев, как и первая компонента. При этом определение самих координат реализовано с помощь генератора псевдослучайных чисел.

Модель функции генерации точек проверки для определения используемой функции встраивания приведена на рисунке 4.43.

```
def Generate_random_checkpoints(Lay_num,num_blocks,block_length,Num_points):
    check=np.zeros([Lay_num,num_blocks,block_length,Num_points,2],dtype=int)
    for i in range(Lay_num):
        for k in range(Num_points):
            for j in range(num_blocks):
                check[i,j,:,k,0]=[random.randint(11-Lay_num+i, 14-Lay_num+i) for _ in range(block_length)]
                check[i,j,:,k,1]=[random.randint(0, block_length-1) for _ in range(block_length)]
    return check
```

Рисунок 4.43 – Модель функции определения точек проверки

Модель функции генерации ключа приведена на рисунке 4.44. Модель функции встраивания с использованием определяемых логических функции на основе математической модели (2.11) приведена на рисунке 4.45.

```
def generate_random_key(Lay_num,num_blocks,block_length):
    key=np.zeros([Lay_num,num_blocks,block_length,2],dtype=int)
    for i in range(Lay_num):
        for j in range(num_blocks):
            key[i,j,:,0]=[random.randint(11-Lay_num+i, 14-Lay_num+i) for _ in range(block_length)]
            key[i,j,:,1]=[random.randint(0, block_length-1) for _ in range(block_length)]
    return key
```

Рисунок 4.44 – Модель функции определения ключа

```
def Stego_block_transform(X,u,LN,l,block_num,key,check,check_num):
    Y=X.copy()
    ii=0
    for i in range(l):
        for j in range(LN):
            check_res=0
            for k in range(check_num):
                if X[check[j,block_num,i,k,1],check[j,block_num,i,k,0]]==1: check_res+=1
            z1=X[key[j,block_num,i,1],key[j,block_num,i,0]]
            if check_res==0 and j<2:
                z2=z1&u[j,ii]
                if z1==0 & z2==0: ii+=1
            elif check_res==check_num and j<2:
                z2=z1|u[j,i]
                if z1==1 & z2==1: ii+=1
            else:
                z2=z1^u[j,i]
                ii+=1
            Y[i,15-LN+j]=z2
    return Y
```

Рисунок 4.45 – Модель функции встраивания

Важно заметить, что влияние алгоритма определения логической функции сильно зависит от количества проверяемых точек. Если их значение мало, то вероятность использования функций И или ИЛИ повышается в то время, как при большом количестве точек проверки данные функции будут использоваться реже. Возможен алгоритм, при котором количество выбираемых точек проверки зависит от слоя встраивания. Рассмотрим работу модели при фиксированном количестве выбираемых точек, независимо от уровня встраивания. На первом этапе определим количество точек, позволяющее получить наилучшую маскировку. В качестве показателя маскировки определим амплитуду первого отсчета гистограммы распределения значений результатов тестирования скользящего окна выборки отсчетов бит последовательности слоя анализируемого объекта.

Очевидно, что влияние количества используемых точек на степень сокрытия в значительной степени определяется конкретным покрывающим объектом. Проведем моделирование на первом рассматриваемом звуковом фрагменте. Исключим два младших слоя, так как в них статистический характер

ПО близок к случайному. На рисунке 4.46 приведен результат моделирования. Первая зависимость соответствует амплитуде первого столбца гистограммы результатов первого теста четвертого уровня стегосистемы. Второй график – амплитуда для четвертого уровня ПО. Третий и четвертый графики соответствуют третьему битовому уровню. Видно, что с ростом значения NP амплитуда первого столбца падает. Это объясняется тем, что с ростом количества точек выборке снижается вероятность выборки всех нулевых или всех единичных значений, то есть, логические функции И и ИЛИ используются все реже. По графику видно, что для данного ПО Наиболее удачным выглядит NP=5, так как в этом случае значения близки к уровню исходного ПО. На рисунке 4.47 приведен результат анализа стегосистемы и ПО, как на рисунке 4.42. Видно, что графики похожи.

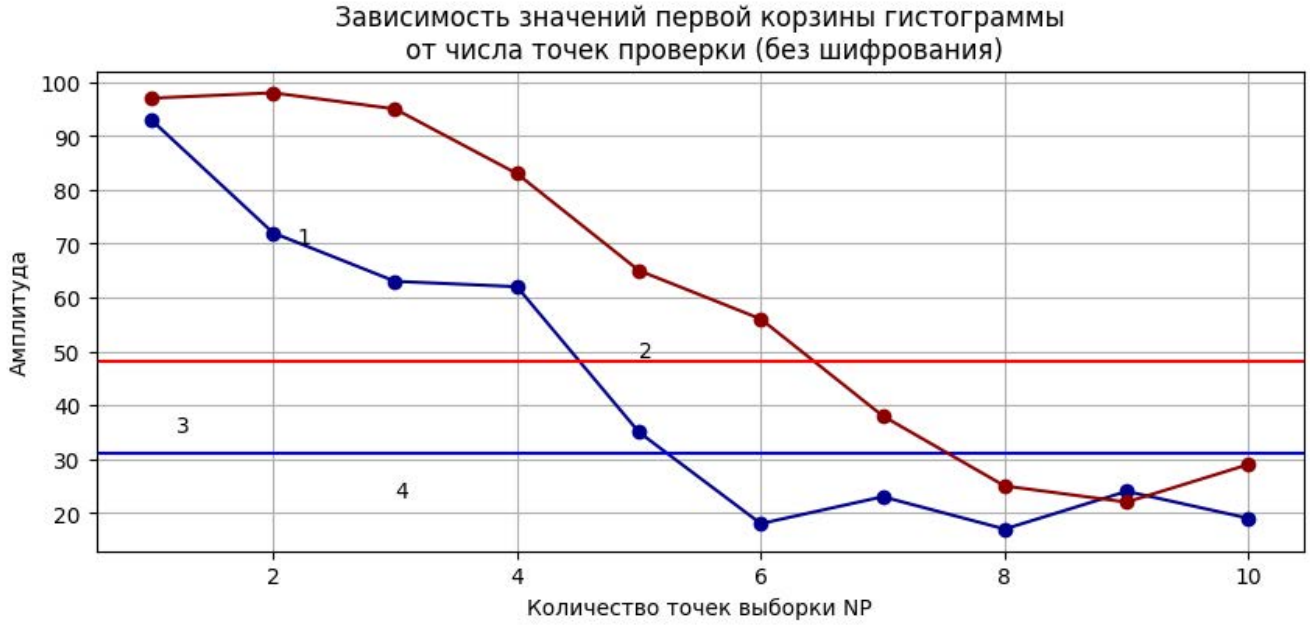


Рисунок 4.46 – Зависимость величины первого столбца гистограммы распределения результатов первого теста в зависимости от количества точек проверки: 1 – Зависимость для 4 уровня стегосистемы; 2 – Амплитуда для 4 уровня ПО; 3– Зависимость для 3 уровня стегосистемы; 4 – Амплитуда 3 уровня ПО

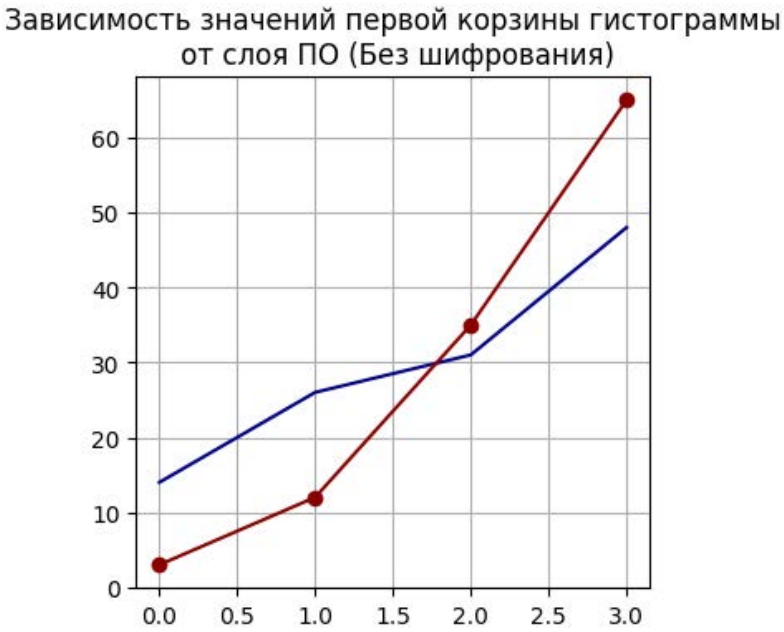


Рисунок 4.47 – Зависимость амплитуды первого столбца гистограммы распределения результатов первого теста музыкального фрагмента от битового слоя

Рассмотрим влияние подстройки на зашифрованные данные. На рисунке 4.48 приведен результат моделирования с зашифрованными шифром AES данными. Первая зависимость соответствует амплитуде первого столбца гистограммы результатов первого теста четвертого уровня стегосистемы. Второй график – амплитуда для четвертого уровня ПО. Третий и четвертый графики соответствуют третьему битовому уровню. Видно, что с ростом значения NP амплитуда первого столбца падает. По графику видно, что для данного ПО Наиболее удачным выглядит NP=5, что полностью совпадает с моделью, использующей незашифрованные данные. На рисунке 4.49 приведен результат анализа стегосистемы и ПО.

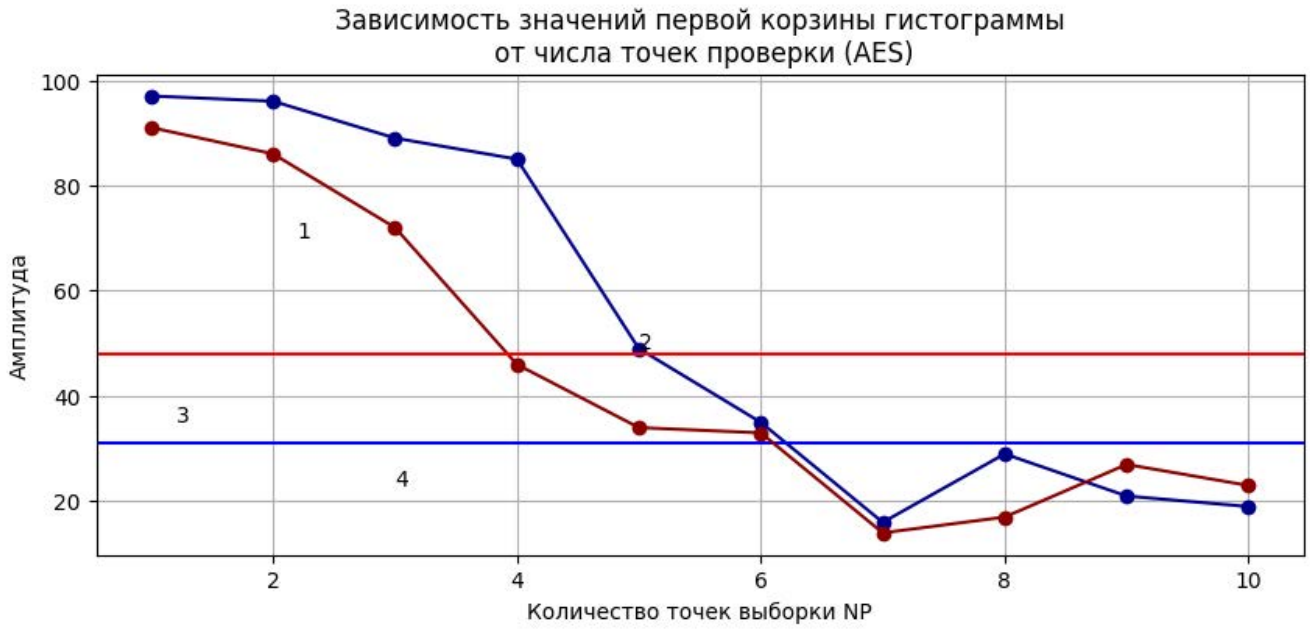


Рисунок 4.48 – Зависимость величины первого столбца гистограммы распределения результатов первого теста в зависимости от количества точек проверки: 1 – Зависимость для 4 уровня стегосистемы; 2 – Амплитуда для 4 уровня ПО; 3– Зависимость для 3 уровня стегосистемы; 4 – Амплитуда 3 уровня ПО

Таким образом, параметры настройки алгоритма встраивания определяются в большей степени параметрами ПО. Это следует из того, что и шифрование, и использование двухкомпонентного контейнера формируют потоки данных, статистические характеристики которых близки к псевдослучайным.

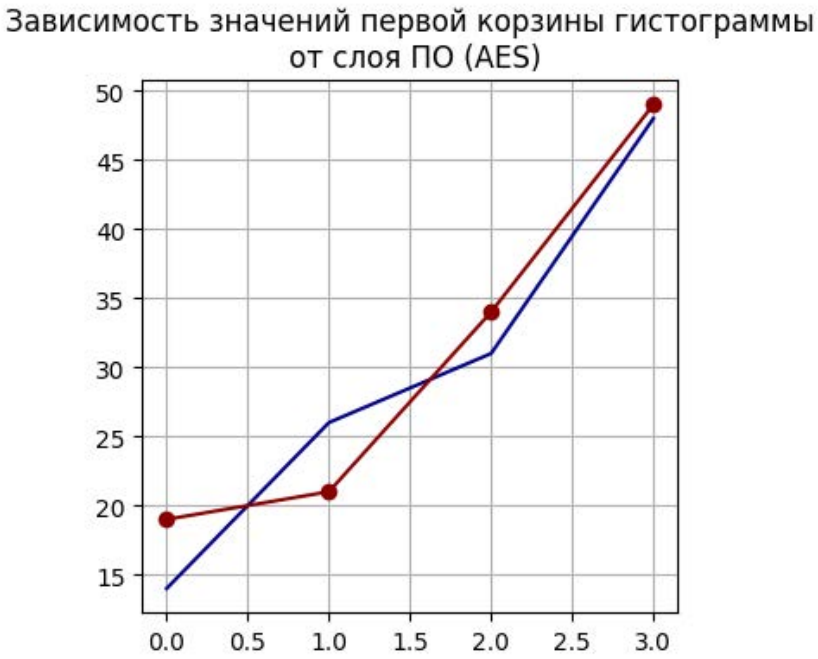


Рисунок 4.49 – Зависимость амплитуды первого столбца гистограммы распределения результатов первого теста музыкального фрагмента от битового слоя

Рассмотрим второй музыкальный фрагмент. На рисунке 4.50 приведен график зависимости величины первого столбца гистограммы распределений результатов первого теста ПО и стегосистемы без шифрования в зависимости от уровня битового слоя. График с маркерами соответствует битовым слоям ПО. Видно, что статистический характер ПО не соответствует статистическому характеру встраиваемых данных. На рисунке 4.51 приведен результат моделирования. Первая зависимость соответствует амплитуде первого столбца гистограммы результатов первого теста четвертого уровня стегосистемы. Второй график – амплитуда для четвертого уровня ПО. Третий и четвертый графики соответствуют третьему битовому уровню.

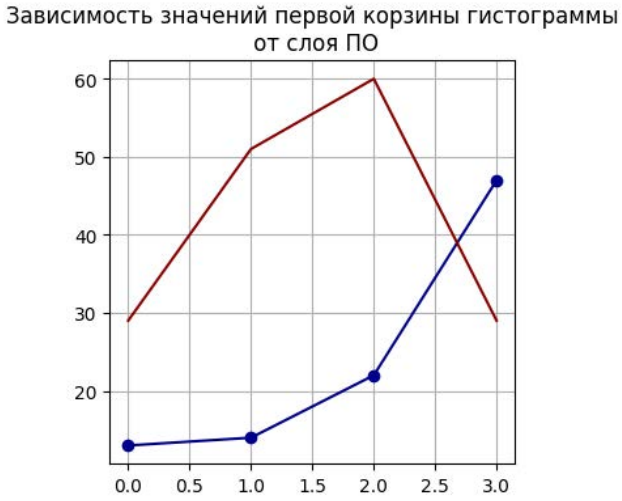


Рисунок 4.50 – Зависимость амплитуды первого столбца гистограммы распределения результатов первого теста музыкального фрагмента от битового слоя



Рисунок 4.51 – Зависимость величины первого столбца гистограммы распределения результатов первого теста в зависимости от количества точек проверки: 1 – Зависимость для 4 уровня стегосистемы; 2 – Амплитуда для 4 уровня ПО; 3– Зависимость для 3 уровня стегосистемы; 4 – Амплитуда 3 уровня ПО

Рассмотрим влияние подстройки на зашифрованные данные. На рисунке 4.52 приведен результат моделирования с зашифрованными шифром AES данными. Первая зависимость соответствует амплитуде первого столбца гистограммы результатов первого теста четвертого уровня стегосистемы. Второй график – амплитуда для четвертого уровня ПО.



Рисунок 4.52 – Зависимость величины первого столбца гистограммы распределения результатов первого теста в зависимости от количества точек проверки: 1 – Зависимость для 4 уровня стегосистемы; 2 – Амплитуда для 4 уровня ПО; 3– Зависимость для 3 уровня стегосистемы; 4 – Амплитуда 3 уровня ПО.

По рисункам 4.51 и 4.52 можно заключить, что хорошим вариантом является выбор NP=3 (NP=2 при отсутствии шифрования дает излишне большое значение). На рисунке 4.53 приведен результат анализа стегосистемы и ПО без шифрования для NP=3. На рисунке 4.54 приведен результат анализа стегосистемы и ПО с шифрованием AES для NP=3. Видно, что статистических характер стегосистемы соответствует статистическому характеру ПО.

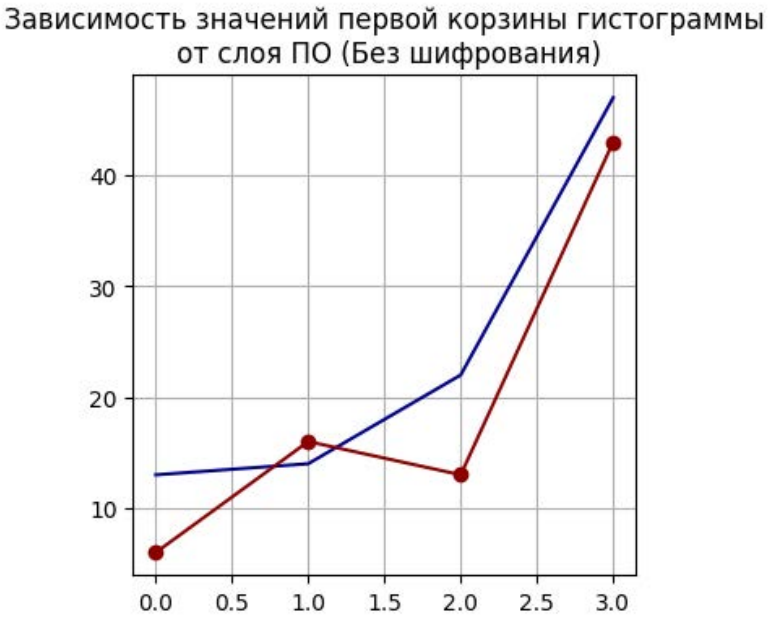


Рисунок 4.53 – Зависимость амплитуды первого столбца гистограммы распределения результатов первого теста музыкального фрагмента от битового слоя

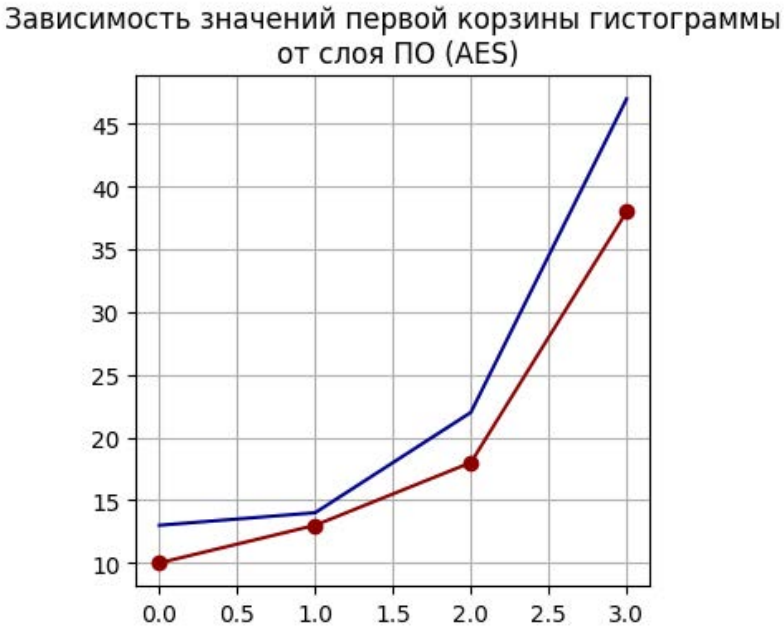


Рисунок 4.54 – Зависимость амплитуды первого столбца гистограммы распределения результатов первого теста музыкального фрагмента от битового слоя

Сравнивая с первым фрагментом видно, что в данном случае NP изменилось. Тем не менее, исходя из условия, что при встраивании информации оригинальные слои ПО удаляются, важно, чтобы встроенные данные имели «формальное» сходство с ПО, то есть имели статистическую зависимость близкую к экспоненциальной. При этом, учитывая многообразие данных, выбирать малое значение NP нецелесообразно, так как это вызовет чрезмерное искажение статистических свойств стегосистемы.

Очевидно, что полученный алгоритм обеспечивает высокий уровень маскировки, при стеганографическом анализе статистических свойств стегосистемы по битовым слоям. Получим результаты численного анализа результатов с помощью коэффициента корреляции Пирсона. Проанализируем значения, приведенные на рисунках 4.50, 4.53 и 4.54. Коэффициент корреляции между характеристиками ПО и данными сообщения. Полученные результаты приведены на рисунке 4.55.

```
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 4.55 – Результат анализа моделирования.

Анализ результатов моделирования показывает, что коэффициент корреляции Пирсона результатов встраивания с использованием функции адаптации алгоритма близок к единице (более 0,9), что по отношению к встраиванию исходных данных (коэффициент корреляции менее 0,4) показывает высокую эффективность маскировки.

Таким образом, можно сделать вывод, что предлагаемый метод позволяет обеспечить высокий уровень маскировки. Однако, значение параметра NP, обеспечивающего наилучший результат определить достаточно сложно, поэтому оно должно выбираться в зависимости от типа звука, используемого в качестве ПО.

4.4. Перспективы развития научного направления

Разработанные в диссертации методы и алгоритмы обладают значительным потенциалом для практического применения и дальнейшего совершенствования. Наиболее востребованными направлениями развития представляются:

1. **Адаптация под речевые аудиокодеки.** Практическая ценность данного направления обусловлена необходимостью защиты речевого трафика в современных системах IP-телефонии и видеоконференцсвязи, где применяются специализированные кодеки с жесткими ограничениями на скорость передачи.

2. **Разработка систем стегоанализа.** Построение системы стегоанализа на основе предложенной методики визуально-численного анализа откроет возможности для создания средств контроля и аудита стеганографических каналов, что востребовано в задачах обеспечения информационной безопасности.

3. **Расширение адаптивных возможностей системы.** Исследование других функций адаптации позволит создать систему, способную эффективно функционировать в широком диапазоне условий — от идеальных каналов до каналов с высоким уровнем шумов и активным противодействием.

Выводы по четвертой главе

В четвертой главе проведено численное моделирование разработанных алгоритмов и применение методик оценки свойств стегосистем. Численное моделирование в среде Python проведено для всех рассматриваемых в работе алгоритмов. Причем алгоритмы на основе многоуровневого встраивания зарегистрированы, как программы ЭВМ [45]. Показано, что все теоретические положения справедливы. Модели реализовывались для различных ПО и для данных, представленных в зашифрованном и в незашифрованном виде.

Рассмотрены алгоритмы встраивания, как в младший битовый слой, так и многоуровневое встраивание в несколько битовых слоев звукового ПО. Причем, многоуровневое встраивание производилось, как для алгоритма без адаптации, так и для алгоритма с адаптацией стегосистемы к статистическим свойствам ПО.

Эксперимент подтвердил, что использование адаптации стегосистемы за счет использования выбираемых логических функций связи компонент, позволяет получить улучшенную маскировку информации в старших битовых слоях [3].

Заключение

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 слоев 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 счет 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 результаты позволяют повысить эффективность защиты встраиваемой информации с помощью инвариантных систем стеганографической защиты информации в реальном времени для звуковых покрывающих объектов, за счет повышения сокрытия и повышения сложности извлечения сообщения.

Полученные результаты переданы в организации для внедрения.

Список литературы

1. *Ахрамеева, К.А.* Обнаружение видео стегосистем с использованием универсального метода, основанного на использовании NIST-тестов / К.А. Ахрамеева, В.И. Коржик, З.К. Нгуен // Труды учебных заведений связи. – 2020. – Т. 6. – № 1. – С. 70-76.

2. *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.

3. *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.

4. *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.

5. *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.

6. *Волосатова, Т.М.* Стенографическое сокрытие текстовых данных в аудиофайле-контейнере методом LSB / Т.М. Волосатова, Е.А. Данилина // Технологии инженерных и информационных систем, №4, 2015. – С. 8-15.

7. *ГОСТ 34.12—2018* «Информационная технология. Криптографическая защита информации. Блочные шифры».

8. *Грибунин, В.Г.* Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев // - М.: Солон-Пресс, 2002. – 260 с.

9. *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 2023 года. – Самара: Поволжский государственный университет телекоммуникаций и информатики, 2023. – С. 77-78.

10. *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.

11. *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.

12. *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.

13. *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.

14. *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.

15. *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.

16. *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.

17. *Конахович, Г.Ф.* Компьютерная стеганография. Теория и практика/ Г.Ф. Конахович, А.Ю. Пузыренко // - К.: «МК-пресс», 2006. – 288 с.

18. *Коржик, В.И.* Основы криптографии / В. И. Коржик, Яковлев В.А. – СПб, ИЦ Интермедия. – СПб., 2016. – 295 с.

19. *Коржик, В.И.* Синтез высокоскоростных стегоалгоритмов устойчивых к "слепому" стегоанализу / В. И. Коржик, И. А. Федянин, О. Д. Копылова // Вопросы защиты информации, №2, 2014. – С. 51-56.

20. *Коржик, В.И.* Цифровая стеганография: учебник / В.И. Коржик, А.В. Красов // М.: КноРус. – 2023. – 323 стр. – ISBN-13: 978-5-406-10970-0.

21. *Короновский, А.А.* Способ секретной передачи информации / А.А. Короновский, О.И. Москаленко, П.В. Попов, А.Е. Храмов // Патент на изобретение РФ №2295835. МПК H04L9/12, H04K1/02; заявл. 11.03.2005; опубл. 20.03.2007, Бюл. №8.

22. *Кудрина, М.А.* Скрытие информации в аудиофайлах методами стеганографии / М.А. Кудрина, И.Е. Дулимова // Перспективные информационные технологии (ПИТ 2017) : труды Международной научно-технической конференции, Самара, 14–16 марта 2017 года. – Самара: Самарский научный центр РАН, 2017. – С. 236-237.

23. *Кудряшов, Б.Д.* Основы теории кодирования: учеб. пособие / Б.Д. Кудряшов // Санкт-Петербург: БХВ-Петербург. – 2016. – 400 с.: ил. – ISBN-13: 978-5-9775-3527-4.

24. *Нгуен, З.К.* Исследование и разработка универсального метода стегоанализа на основе использования NIST-тестов: диссертация на соискание ученой степени кандидата технических наук: 05.13.19 / Нгуен Зуи Кыонг; [Место защиты: Санкт-Петербургский государственный университет телекоммуникаций им. Проф. М,А, Бонч-Бруевича] – Санкт-Петербург, 2020 – 136 с.

25. *Рябко, Б.Я.* Основы современной криптографии и стеганографии / Б.Я. Рябко, А.Н. Фионов. - М.: Горячая линия - Телеком, 2019. - 232 с.

26. *Шакурский, В.К.* Сжимающие отображения в инвариантных преобразователях и системах стеганографии / В.К. Шакурский, М.В. Шакурский. – Самара : Самарский научный центр РАН, 2014. – 159 с.

27. *Шакурский, М.В.* Алгоритм сокрытия использования двухкомпонентного контейнера в стеганографической системе / М.В.

Шакурский// Журнал Вопросы защиты информации №3 (130) Издательство ФГУП «НТЦ оборонного комплекса «Компас» 2020 г. С. 3-5.

28. *Шакурский, М.В.* Выбор ключа в двухкомпонентных стеганографических системах, использующих взаимное зашумление компонент / М.В. Шакурский// Журнал «Инфокоммуникационные технологии» №2 Том 17.- Самара: Изд-во ПГУТИ, 2019. Стр. 229-233.

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

30. *Шакурский, М.В.* Двухкомпонентная стеганографическая система встраивания информации в звуковой сигнал, работающая в реальном времени / М.В. Шакурский // Журнал «Проблемы информационной безопасности. Компьютерные системы» №2 Издательство: ФГАОУ ВО "Санкт-Петербургский политехнический университет Петра Великого" 2020 г. С. 40-45.

31. *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.

32. *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.

33. *Шакурский, М.В.* Математические модели двухкомпонентных инвариантных стеганографических систем, использующих различные алгоритмы связи встраиваемых сигналов / М.В. Шакурский// Журнал Вопросы защиты информации №2 (121) Издательство ФГУП «НТЦ оборонного комплекса «Компас» 2018 г. С. 3-8

34. *Шакурский, М.В.* Метод встраивания информации в младшие биты растровых изображений без сжатия, использующий двухкомпонентный контейнер / М.В. Шакурский // Журнал Вопросы защиты информации №2 (129) Издательство ФГУП «НТЦ оборонного комплекса «Компас» 2020 г. С. 3-7.

35. *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

36. *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.

37. *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.

38. *Шакурский, М.В.* Оценка стойкости стеганографической системы [Текст] / М.В. Шакурский, В.К. Шакурский // Международный научно-технический журнал «Успехи современной радиоэлектроники». – 2015. – №11. – С. 87-91.

39. *Шакурский, М.В.* 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; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования "Поволжский государственный университет телекоммуникаций и информатики".

40. *Шакурский, М.В.* Свидетельство о государственной регистрации программы для ЭВМ № 2025616230 Российская Федерация. Программа реализации NIST тестов для анализа битных последовательностей: заявл. 28.02.2025: опубл. 13.03.2025 / М. В. Шакурский, О. А. Караулова ; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования "Поволжский государственный университет телекоммуникаций и информатики".

41. *Шакурский, М.В.* Свидетельство о государственной регистрации программы для ЭВМ № 2025615790 Российская Федерация. Программа реализации шифра AES: заявл. 28.02.2025: опубл. 07.03.2025 / М.В. Шакурский, О.А. Караулова; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования "Поволжский государственный университет телекоммуникаций и информатики".

42. *Шакурский, М.В.* Свидетельство о государственной регистрации программы для ЭВМ № 2025615456 Российская Федерация. Программа реализации шифра Кузнечик: заявл. 28.02.2025: опубл. 05.03.2025 / М.В. Шакурский, О.А. Караулова; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования "Поволжский государственный университет телекоммуникаций и информатики".

43. *Шакурский, М.В.* 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; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования "Поволжский государственный университет телекоммуникаций и информатики".

44. *Шакурский, М.В.* Свидетельство о государственной регистрации программы для ЭВМ № 2025693867 Российская Федерация. Программа многослойного встраивания скрываемой информации в биты звукового

покрывающего объекта с использованием двухкомпонентного контейнера: заявл. 17.11.2025: опубл. 02.12.2025 / М.В. Шакурский, О.А. Белова; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования "Поволжский государственный университет телекоммуникаций и информатики".

45. *Шакурский, М.В.* Способ сокрытия информации /М.В. Шакурский, В.Н. Козловский, О.А. Караулова // Пат. 2815915 С1 Российская Федерация, МПК H04L 9/00; заявл. 10.04.2023. 25.03.2024 Бюл. №9.

46. *Шакурский, М.В.* Способ сокрытия информации /М.В. Шакурский, О.А. Белова // Пат. 2859964 С1 Российская Федерация, № 2025127723: заявл. 09.10.2025 : опубл. 14.04.2026.

47. *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.

48. *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.

49. *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.

50. *Шелухин, О.И.* Стеганография. Алгоритмы и программная реализация / О.И. Шелухин, С.Д. Канаев // М.: Горячая Линия – Телеком. – 2021. – 592 стр.

51. *Adhiya, K.P.* Hiding Text in Audio Using LSB Based Steganography / K.P. Adhiya, Swati A. Patil // Information and Knowledge management. Vol. 2, No. 3, 2012. – P. 8-14.

52. *Anderson, R.J.* On the limits of Steganography / R. J. Anderson, F.A.P.Petitcolas // IEEE Journal on Selected Areas in Communications (J- SAC), Special Issue on Copyright and Privacy Protection No. 16. 1998. – P. 474- 481.

53. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / A. Rukhin [et al.]. Gaithersburg: National Institute of Standards and Technology, 2010. 131 p.

54. *Ashwini, M.* Data Hiding Technique: Audio Steganography using LSB Technique / M. Ashwini, G. Gajanan, J. Amutha // International Journal of Engineering Research and Applications. Vol. 2, Issue 3, 2012. – P.1123-1125

55. *Bhavana, S.* Text steganography using LSB insertion method along with Chaos theory / S. Bhavana, K.L. Sudha // International Journal of Computer Science, Engeneering and Applications (IJCSEA). – Vol. 2, No. 2, 2012. – P. 145-149.

56. *Burate, D.J.* Performance Improving LSB Audio Steganography Technique / D.J. Burate, M.R. Dixit // International Journal of Advance Research in Computer Science and Management Studies, 2013, No 1. – P. 67-75.

57. *Chadha, A.* An Efficient Method for Image and Audio Steganography Using Least Significant Bit (LSB) Substitution / A. Chadha, N. Satam, R. Sood, D. Bade // International Journal of Computer Applications, 2013, No. 77. – P. 37-45.

58. *Chaharlang, J.* A novel quantum steganography-Steganalysis system for audio signals / J. Chaharlang, M. Mosleh, S. Rasouli-Heikalabad // Multimed Tools Appl. – 2020.

59. *Chandel, B.* Video steganography: a survey / B. Chandel, Dr. S. Jain // IOSR: Journal of computer engineering Vol. 18, Issue 1, 2016. – P. 11-17.

60. *Chandrakar, P.* Enhancement in Security of LSB Based Audio Steganography Using Multiple Files / P. Chandrakar, M. Choudhary,C. Badgaiyan // International Journal of Computer Applications, 2013, No 73. – P. 21-24.

61. *Cvejic, N.A* wavelet domain LSB Insertion algorithm for high capacity audio Steganography / N. Cvejic, T. Seppanen // Digital Signal Processing Workshop, 2002 and the 2nd Signal Processing Education Workshop. Proceedings. 2002. DOI: 10.1109/DSPWS.2002.1231075.

62. *Cvejic, N.* Increasing robustness of LSB audio steganography by reduced distortion LSB coding / N. Cvejic, T. Seppanen // Proceedings ITCC 2004 International Conference on Information Technology: Coding and Computing, Vol. 2, 2004. – P. 533 – 537.

63. *Cvejic, N.* Increasing Robustness of, LSB Audio Steganography Using a Novel Embedding Method / N Cvejic, T. Seppanen // Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC04). vol. 2, 2004. – P. 533-543. DOI: 10.1109/ITCC.2004.1286709

64. *Cvejic, N.* Increasing the capacity of LSB-based audio steganography /N. Cvejic, T. Seppben // Conference: Multimedia Signal Processing ,2003. – P. 336-338.

65. *Cvejic, N.* Reduced distortion bit-modification for LSB audio steganography / N. Cvejic, T. Seppanen // Journal Universal Computer Sciences No. 11(1), 2005. – P. 56-65.

66. *Dabeer, O.* Detection of Hiding in the Least Significant Bit / O. Dabeer, K. Sullivan, S. Chandrasekaran, B.S. Manjunath // IEEE Transactions on Signal Processing. Vol 52. No. 10. 2004. – P. 3046-3058.

67. *Delforouzi, A.* Adaptive Digital Audio Steganography Based on Integer wavelet transform / A. Delforouzi, M. Pooyan // IEEE Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2007. – P. 283-286.

68. *Dutta, H.* An overview of digital audio steganography / H. Dutta, R.K. Das, S. Nandi, S.M. Prasanna // IETE Technical Review. – 2020. – Vol. 37. – № 6. – pp. 632-650.

69. Federal Information Processing Standards Publication 197 November 26, 2001 Specification for the ADVANCED ENCRYPTION STANDARD (AES).

70. *Fridrich, J.* Practical steganalysis of digital images - state of the art./ J. Fridrich, M. Golijan // Proceedings of SPIE, 2002, vol. 4675. P. 13. doi: 10.1117/12.465263.

71. *Fridrich, J.* Steganalysis of LSB encoding in color images / J. Fridrich, R. Du, M. Long // ICME, 2000. P. 22-28.

72. *Fridrich, J.* Steganography in digital media. Principles, Algorithms and applications / J. Fridrich // Cambridge university press, New York, 2010. – P. 437.

73. *Gadicha, A.B.* Audio Wave Steganography / A.B. Gadicha // International Journal of Soft Computing and Engineering (IJSCE), 2011. No 1. – P. 174-176.

74. *Gupta, S.* Enhanced Least Significant Bit algorithm For Image Steganography / S. Gupta, G. Gujral, N. Aggarwal// International Journal of Computer Engeneering & Management, Vol. 15. Issue 4, 2012. – P. 40-42.

75. *Han, C.* A new audio steganalysis method based on linear prediction / C. Han, R. Xue, R. Zhang, X. Wang // Multimedia Tools and Applications. – 2018. – Vol. 77. – № 12. – pp. 15431-15455.

76. *Hassan, M.D.* Sound based Steganalysis for Waveform Audio File Format (WAV) and Audio File Format (AU) / M.D. Hassan, M.A.M. Amin, S. Mahdi // Journal of Electronic Systems Volume. – 2018. – Vol. 8. – № 3. – pp. 103-111.

77. *Hasso, S.* A-R. Steganography in video files / Sahd Abdul-Rhman Hasso // International journal of computer science issues, Vol. 13, Issue 1, 2016. – P. 32-35.

78. *Huang Xuping* The Real-Time Steganography Based on Audio-to-Audio Data Bit Stream / Xuping Huang, Ryota Kawashima, Norihisa Segawa, Yoshihiko Abe // Technical report of The Institute of Electronics, Information and Communication Engineers, ISEC, Vol.106, 2006. – P.15-22.

79. *Jayaram, P.* Information Hiding Using Audio Steganography—A Survey. / P. Jayaram, H.R. Ranganatha, H.S. Anupama // The International Journal of Multimedia & Its Applications (IJMA), Vol. 3, 2011. – P. 86-96.

80. *Johnson, N.F.* Information Hiding Steganography and Watermarking-Attacks and Countermeasures / N. Johnson, Z. Duric, S. Jajodia // Kluwer Academic Publishers, 2001. – P. 129.

81. *Juneja, M.* Application of LSB Based Steganographic Technique for 8-bit Color Images / M. Juneja, P.S. Sandhu, E. Walia // International Journal of Computer, Electrical, Automation, Control and Information Engineering, and Technology, Vol.3, No. 2, 2009. – P. 297-299.

82. *Kamred Udham Singh* Video steganography: text hiding in video by LSB substitution / Kamred Udham Singh// International journal of engineering research and applications, Vol. 4, Issue 5, 2014. – P. 105-108.

83. *Kekre, H.B.* Increasing the capacity of the cover audio signal by using multiple LSBs for information hiding / H.B. Kekre , Archana Athawale, B. Swarnalata Rao, Uttara Athawale // IEEE Third International Conference on Emerging Trends in Engineering and Technology, 2010. DOI: 10.1109/ICETET.2010.118.

84. *Kexin, Z.* Audio steganalysis of spread spectrum hiding based on statistical moment / Z. Kexin // 2010 2nd International Conference on Signal Processing Systems. – Dalian, China. – 2010. – pp. V3-381-V3-384.

85. *Krenn, R.* Steganography and steganalysis / R. Krenn //, An Article, 2004. URL: http://www.krenn.nl/univ/cry/steg/article.pdf

86. *Kumar, S.* LSB Modification and Phase Encoding Technique of Audio Steganography Revisited / S. Kumar, B. Barnali, G. Banik // International Journal of Advanced Research in Computer and Communication Engineering, 2012, No. 1. – P. 1-4.

87. *Liu, Q.* Derivative-based audio steganalysis / Q. Liu, A.H. Sung, M. Qiao // ACM Transactions on Multimedia Computing, Communications, and Applications. – 2011. – Vol. 7. – № 3. – pp. 1-18.

88. *Lokeswara, R.V.* Implementation of LSB Steganography and its Evaluation for Various File Formats / V. Lokeswara Reddy, Dr.A.Subramanyam, Dr.P. Chenna Reddy // International Journnal of Advanced Networking and Applications, Vol. 2, Issue 5, 2011. – P. 868-872.

89. *Mengyu Qiao* Feature Mining and Intelligent Computing for MP3 Steganalysis / Mengyu Qiao, Andrew H. Sung , Qingzhong Liu // International Joint

Conference on Bioinformatics, Systems Biology and Intelligent Computing 2009. DOI: 10.1109/IJCBS.2009.119

90. *Mennatallah M.* Sadek Video steganography: a comprehensive review / Mennatallah M. Sadek, Amal S. Khalifa, Mostafa G. M. Mostafa // Multimedia tools and applications Vol. 74, Issue 17, 2015. – P. 7063–7094.

91. *Mohd, B.J.* FPGA Hardware of the LSB Steganography Method / B.J. Mohd, S. Abed, and T. Hayajneh, S. Alouneh // Computer, Information and Telecommunication Systems (CITS) 2012. DOI: 10.1109/CITS.2012.6220393

92. *Morkel, T.* An Overview of Image Steganography / T Morkel, J.H.P. Eloff, M.S Olivier // Proceeding of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sand to South Africa, 2005. – P. 12.

93. *Mrs. Kavitha* Steganography Using Least Significant Bit Algorithm / Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav // International Journal of Engineering Research and applications, Vol.2, Issue 3, 2012. – P. 338-341.

94. *Naofumi, A.* A Band Widening Technique for VoIP Speech Using Steganography Technology / A. Naofumi //, Report of Institute of Electronics, Information and Communication Engineers, SP,106(333), 2006. – P.31-36.

95. *Neeta, D.* Implementation of LSB Steganography and Its Evaluation for Various Bits/ D. Neeta, K. Snehal, D. Jacobs//, Digital Information Management, 2006 1st International Conference, 2007. DOI: 10.1109/ICDIM.2007.369349.

96. *Pooyan, M.* LSB-based Audio Steganography Method Based on Lifting Wavelet Transform / M. Pooyan, A. Delforouzi //, Proceedings of 7th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT'07), 2007. DOI**:** 10.1109/ISSPIT.2007.4458198

97. *Qi, Y.* Wavelet domain audio steganalysis based on statistical moments of histogram / Y. Qi, J. Fu, J. Yuan // Journal of System Simulation. Vol 20, No. 7. 2008. – P. 1912-1914.

98. *Ramesh, Y.P.* Hiding Data in Audio Using Audio Steganography / P. Ramesh Yadav, V. Usha Shree, K. Padmapriya //, International Journal of Computer Applications in Engineering Sciences, Vol. 1, Issue 2, 2011. – P. 207-211.

99. *Roque, J.J.* SLSB: Improving the steganographic algorithm LSB / J. J. Roque, J. M. Minguet // Proceedings The Ibero-American Congress on Information Security (CIBSI), 2009. – P. 398-408.

100. *Roque, J.J.* SLSB: Improving the Steganographic Algorithm LSB / J. J. Roque, J. M. Minguet // 7th International Workshop on Security in Information Systems (WOSIS 2009), Milan, Italy, 2009. – P.1-11.

101. *Shakurskiy, M.V.* Computer model of steganographic system based on contraction mapping with stream audio container / M.V. Shakurskiy, V.K. Shakurskiy, V.I. Volovach // Proceedings of IEEE East-West Design & Test Symposium (EWDTS'2015) / KNURE, Kharkov 2015 p. 306-309.

102. *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.

103. *Shakurskiy, M.V.* Two-channel real-time steganographic system / M.V. Shakurskiy, V.K. Shakurskiy, V.I. Volovach // Proceedings of IEEE East-West Design & Test Symposium (EWDTS'2014) / KNURE, Kharkov 2014 p. 309-311.

104. *Sheikhan, M.* High Quality Audio steganography by Floating Substitution of LSBs in Wavelet Domain / M. Sheikhan, K. Asadollahi, E. Hemmati // World Applied Science Journal. Vol. 10, Issue 12, 2010. – P. 1501-1507.

105. The Transport Layer Security (TLS) Protocol Version 1.3 /E. Rescorla // Internet Engineering Task Force (IETF), 2018. URL: https://datatracker.ietf.org/doc/html/rfc8446

106. *Wakiyama, M.* An audio steganography by a low-bit coding method with wave files / M. Wakiyama, Y. Hidaka, K. Nozaki // IEEE 2010 Sixth International Conferene on Intelligent Information Hiding and Multimedia Signal Processing, 2010. DOI: 10.1109/IIHMSP.2010.135

107. *Walia, E.* An Analysis of LSB & DCT based Steganography / E. Walia, P. Jain, N. Navdeep // Global Journal of Computer Science and Technology, Vol. 10, 2010. – P. 4-8.

108. *Wei, Y.* A blind audio steganalysis based on feature fusion / Y. Wei, L. Guo, Y. Wang, C. Wang // Journal of Electronics (China). – 2011. – Vol. 28. – № 3. – pp. 265-276.

109. *Westfeld, A.* Attacks on Steganographic Systems / A. Westfeld, A. Pfitzmann // A. Pfitzmann (eds) Information Hiding. IH 1999. Lecture Notes in Computer Science. – Springer, Berlin, Heidelberg. – 1999. – Vol. 1768.

110. *Zeng, W.* Audio steganalysis of spread spectrum information hiding based on statistical moment and distance metric / W. Zeng, R. Hu, H. Ai // Multimedia Tools and Applications. – 2011. – Vol. 55. – № 3. – pp. 525-556.

Приложение 1. Акты внедрения результатов диссертационного исследования

Поволжский государственный
УНИВЕРСИТЕТ
СЕРВИСА

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное
образовательное учреждение высшего образования
«Поволжский государственный университет сервиса»
(ФГБОУ ВО «ПВГУС»)

УТВЕРЖДАЮ
Проректор ФГБОУ ВО «ПВГУС»
_____ А.Н. Попов
«19» _____ 2025 г.

АКТ

19.12.25 № 614

г. Тольятти

об использовании результатов
диссертационного исследования в учебном процессе
Высшей школы интеллектуальных систем и кибертехнологий

С 2024-2025 учебного года в учебный процесс Высшей школы интеллектуальных систем и кибертехнологий федерального государственного бюджетного образовательного учреждения высшего образования «Поволжский государственный университет сервиса» на основании решения Высшей школы интеллектуальных систем и кибертехнологий (протокол № 4 от 15.11.2024 г.). были внедрены результаты диссертационного исследования Беловой Ольги Александровны. на тему: **«Инвариантные системы стеганографической защиты информации в реальном времени для звуковых покрывающих объектов»**.

Представленные ниже результаты диссертационного исследования:

1. Алгоритм многоуровневого встраивания информации в звуковой покрывающий объект.
2. Математические модели двухкомпонентных стеганографических систем для встраивания сообщений, как в младший битовый слой, так и для многоуровневого встраивания информации.
3. Структурные схемы встраивания битов сообщения в отсчеты покрывающего объекта.
4. Имитационные модели разработанных стеганографических систем в среде Python.

используются в курсах дисциплин «Защита информации от утечки по техническим каналам» и «Методы и средства технической защиты информации» направлений подготовки 10.03.01 «Информационная безопасность» и 10.04.01 «Информационная безопасность».

Директор Высшей школы
интеллектуальных систем и
кибертехнологий к.э.н., доцент _____ О.А. Филиппова

АКТ
о практическом применении результатов диссертационного исследования Беловой Ольги Александровны на тему «Инвариантные системы стеганографической защиты информации в реальном времени для звуковых покрывающих объектов»,
о внедрении результатов диссертационной работы

ООО «Идентификация» специализируется на реализации мер технической защиты информации, включая обследование помещений, установку и сертификацию специализированного программного обеспечения.

В рамках проекта по поиску скрытых каналов утечки информации научные результаты, полученные в работе Беловой О.А. представляют практический интерес

Настоящим Актом удостоверяется, что Беловой О.А. переданы следующие результаты диссертационного исследования:

1. Математические модели многослойной стеганографической системы.
2. Программные реализации многослойных стеганографичнских систем.
3. Методика анализа битовых последовательностей для поиска скрытых данных в звуке.

Предложенный способ формирования стеганографической системы и ее обнаружения положен в основу работы по развитию систем поиска скрытых каналов утечки информации. Использование предложенных решений позволило повысить полезную нагрузку при встраивании более чем в 2 раза по отношению к известным методам.

Генеральный директор ООО «Идентификация» С.А. Глубоков
«22.06.2026»

УТВЕРЖДАЮ

Проректор по учебной работе
ФГБОУ ВО ПГУТИ
д.т.н., доцент

_____ Буранова М.А.

«10» 04 2026 г.

АКТ

о внедрении результатов диссертационной работы Беловой О.А.

«Инвариантные системы стеганографической защиты информации в реальном времени для звуковых покрывающих объектов»

Комиссия ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики» в составе: председателя комиссии Тучковой А.С. – начальника управления организации учебного процесса (УОУП), и членов комиссии: д.т.н., доц. Шакурского М.В. – заведующего кафедрой информационной безопасности (ИБ), к.т.н., Поздняк И.С. – декана 1 Факультета, к.т.н., доц., составили настоящий акт о том, что в университете внедрены в учебный процесс на кафедре ИБ следующие результаты диссертационной работы Беловой О.А.:

Внедрение осуществлено в следующем виде:

1. Разработанная в диссертации методика оценки процессов стеганографической защиты информации в цифровых звуковых сигналах, обрабатываемых в реальном времени используется в лекционном курсе по дисциплине «Прикладные методы теории случайных функций в защищенных системах связи» для студентов направления подготовки 10.03.01 Информационная безопасность.

2. Результаты исследования, а именно результаты компьютерного моделирования стеганографических преобразований, полученные в ходе численных экспериментов в среде Python внедрены в практические занятия и используются при подготовке для студентов направлению подготовки 10.03.01 Информационная безопасность.

3. Разработанные материалы способствуют повышению уровня подготовки обучающихся, развитию практических навыков анализа систем защиты информации, использующие стеганографические технологии.

Заключение:

Результаты диссертации Беловой О.А. представляют научную и практическую ценность, их использование повышает качество преподавания дисциплин

Председатель комиссии:
Начальника УОУП А.С. Тучкова

Члены комиссии:
Зав. кафедрой ИБ
д.т.н., доц. М.В. Шакурский

Декан 1 Факультета
к.т.н., доц. И.С. Поздняк

Приложение 2. Полученные патенты и свидетельства о регистрации программ для ЭВМ и электронных ресурсов



РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ИЗОБРЕТЕНИЕ
№ 2815915

Способ сокрытия информации

Патентообладатель: ***Федеральное государственное бюджетное образовательное учреждение высшего образования "Поволжский государственный университет телекоммуникаций и информатики" (RU)***

Авторы: ***Шакурский Максим Викторович (RU), Козловский Владимир Николаевич (RU), Караулова Ольга Александровна (RU)***

Заявка № **2023108967**
Приоритет изобретения **10 апреля 2023 г.**
Дата государственной регистрации
в Государственном реестре изобретений
Российской Федерации **25 марта 2024 г.**
Срок действия исключительного права
на изобретение истекает **10 апреля 2043 г.**

Руководитель Федеральной службы
по интеллектуальной собственности

Ю.С. Зубов

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ИЗОБРЕТЕНИЕ

№ 2859964

Способ сокрытия информации

Патентообладатель: ***Федеральное государственное бюджетное образовательное учреждение высшего образования "Поволжский государственный университет телекоммуникаций и информатики" (RU)***

Авторы: ***Шакурский Максим Викторович (RU), Белова Ольга Александровна (RU)***

Заявка № **2025127723**
Приоритет изобретения **09 октября 2025 г.**
Дата государственной регистрации
в Государственном реестре изобретений
Российской Федерации **14 апреля 2026 г.**
Срок действия исключительного права
на изобретение истекает **09 октября 2045 г.**

Руководитель Федеральной службы
по интеллектуальной собственности

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 00a570e4f7add8d531b4b8818e75f29506
Владелец **Зубов Юрий Сергеевич**
Действителен с 04.09.2025 по 28.11.2026

Ю.С. Зубов

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2023610522

Программа реализации инвариантной системы стеганографической защиты информации в реальном времени с использованием двухкомпонентных контейнеров для звукового сигнала WAVE

Правообладатель: ***Федеральное государственное бюджетное образовательное учреждение высшего образования "Поволжский государственный университет телекоммуникаций и информатики" (RU)***

Авторы: ***Шакурский Максим Викторович (RU), Караулова Ольга Александровна (RU)***

Заявка № **2022685387**
Дата поступления **21 декабря 2022 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***11 января 2023 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Ю.С. Зубов

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2025616230

Программа реализации NIST тестов для анализа битных последовательностей

Правообладатель: ***Федеральное государственное бюджетное образовательное учреждение высшего образования "Поволжский государственный университет телекоммуникаций и информатики" (RU)***

Авторы: ***Шакурский Максим Викторович (RU), Караулова Ольга Александровна (RU)***

Заявка № **2025614007**
Дата поступления **28 февраля 2025 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***13 марта 2025 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Ю.С. Зубов

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2025615456

Программа реализации шифра Кузнечик

Правообладатель: ***Федеральное государственное бюджетное образовательное учреждение высшего образования "Поволжский государственный университет телекоммуникаций и информатики" (RU)***

Авторы: ***Шакурский Максим Викторович (RU), Караулова Ольга Александровна (RU)***

Заявка № **2025613992**
Дата поступления **28 февраля 2025 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***05 марта 2025 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Ю.С. Зубов

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2025615790

Программа реализации шифра AES

Правообладатель: ***Федеральное государственное бюджетное образовательное учреждение высшего образования "Поволжский государственный университет телекоммуникаций и информатики" (RU)***

Авторы: ***Шакурский Максим Викторович (RU), Караулова Ольга Александровна (RU)***

Заявка № **2025614010**
Дата поступления **28 февраля 2025 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***07 марта 2025 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Ю.С. Зубов

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2025694027

Программа оконного встраивания скрываемой информации в младшие биты звукового покрывающего объекта с использованием двухкомпонентного стеганографического контейнера

Правообладатель: ***Федеральное государственное бюджетное образовательное учреждение высшего образования "Поволжский государственный университет телекоммуникаций и информатики" (RU)***

Авторы: ***Шакурский Максим Викторович (RU), Белова Ольга Александровна (RU)***

Заявка № **2025692866**

Дата поступления **17 ноября 2025 г.**

Дата государственной регистрации в Реестре программ для ЭВМ ***03 декабря 2025 г.***

Руководитель Федеральной службы по интеллектуальной собственности

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 00a570e4f7add8d531b4b8818e75f29506
Владелец **Зубов Юрий Сергеевич**
Действителен с 04.09.2025 по 28.11.2026

Ю.С. Зубов

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2025693867

Программа многослойного оконного встраивания скрываемой информации в биты звукового покрывающего объекта с использованием двухкомпонентного стеганографического контейнера

Правообладатель: ***Федеральное государственное бюджетное образовательное учреждение высшего образования "Поволжский государственный университет телекоммуникаций и информатики" (RU)***

Авторы: ***Шакурский Максим Викторович (RU), Белова Ольга Александровна (RU)***

Заявка № **2025692855**

Дата поступления **17 ноября 2025 г.**

Дата государственной регистрации в Реестре программ для ЭВМ ***02 декабря 2025 г.***

Руководитель Федеральной службы по интеллектуальной собственности

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 00a570e4f7add8d531b4b8818e75f29506
Владелец **Зубов Юрий Сергеевич**
Действителен с 04.09.2025 по 28.11.2026

Ю.С. Зубов

Приложение 3. Результаты экспериментов

П 3.1 Тестирование музыкальных фрагментов при встраивании двух компонент в пределах одного отсчета с использованием функции исключающего ИЛИ

Результат проведения второго теста.

Первый музыкальный фрагмент.

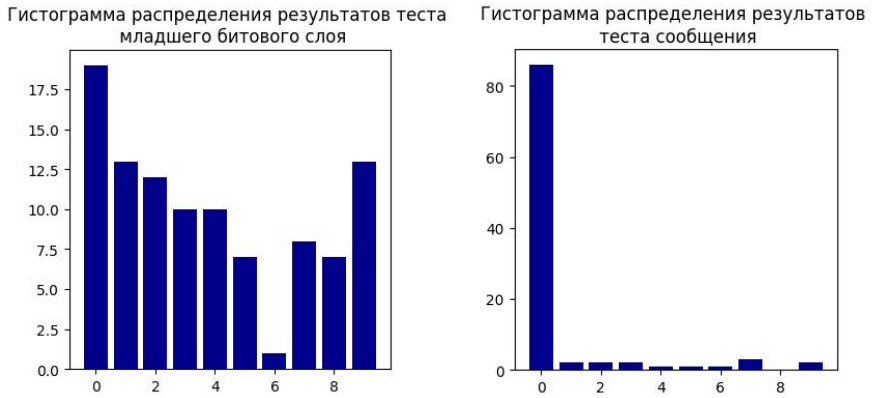


Рисунок П3.1 – Распределения значений результатов тестирования младшего битового слоя первого музыкального фрагмента и сообщения

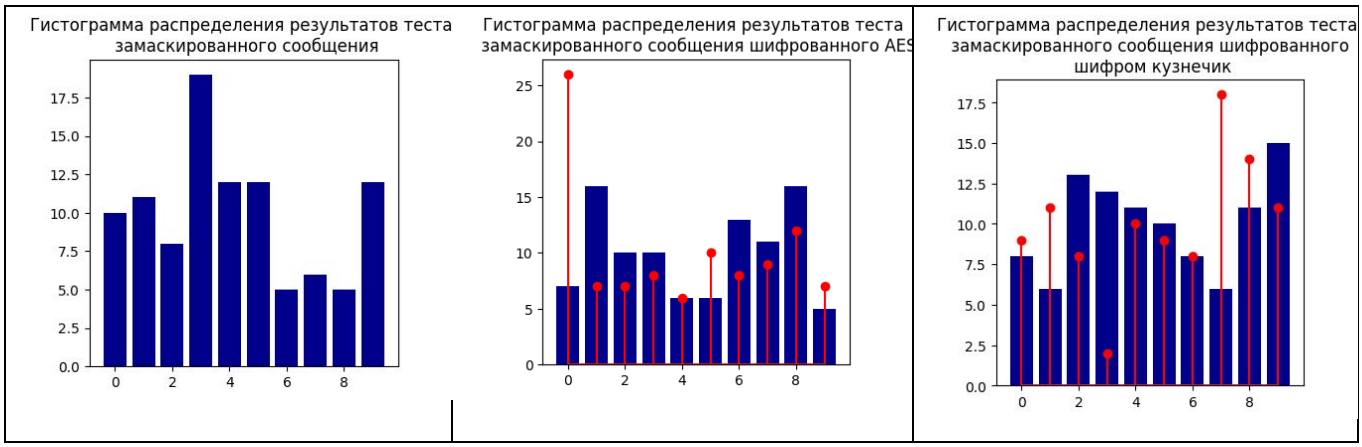


Рисунок П3.2 – Распределения значений результатов тестирования стегосистем первого музыкального фрагмента вторым тестом.

Второй музыкальный фрагмент.



Рисунок П3.3 – Распределения значений результатов тестирования младшего битового слоя второго музыкального фрагмента

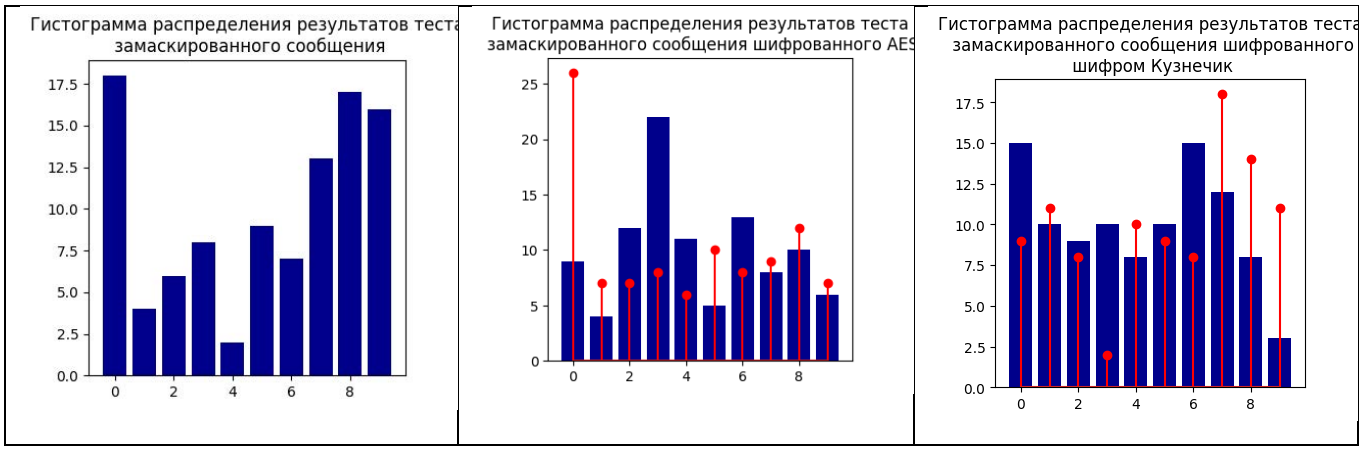


Рисунок П3.4 – Распределения значений результатов тестирования стегосистем второго музыкального фрагмента вторым тестом.

Третий музыкальный фрагмент

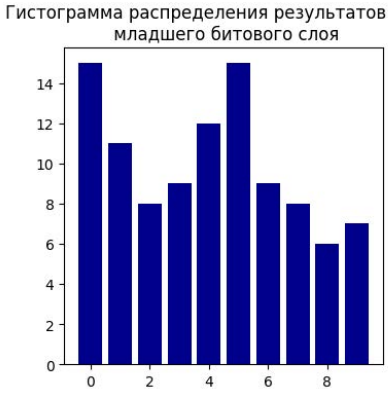


Рисунок П3.5 – Распределения значений результатов тестирования младшего битового слоя третьего музыкального фрагмента

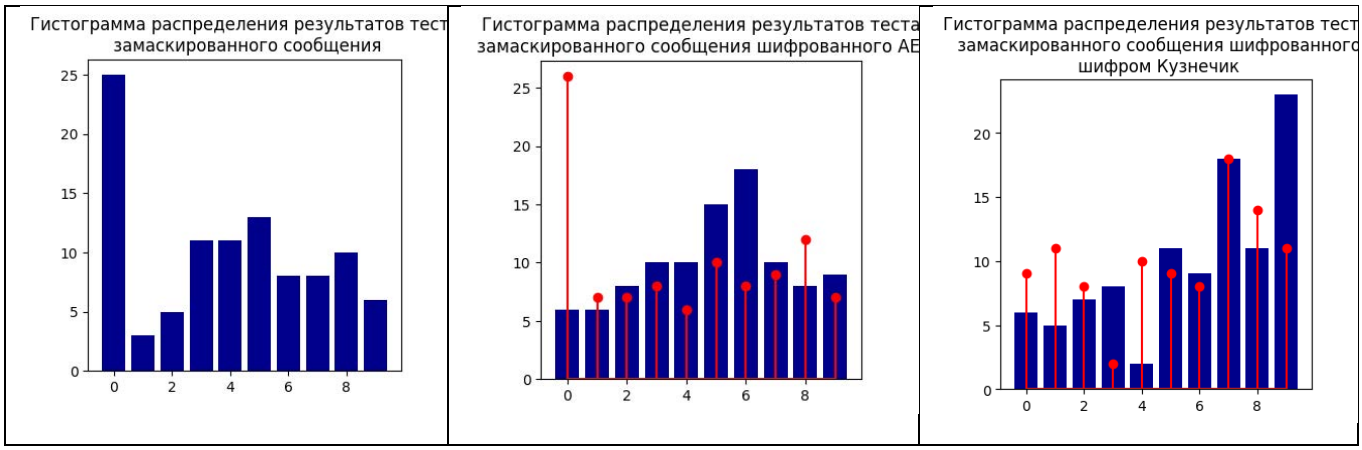


Рисунок П3.6 – Распределения значений результатов тестирования стегосистем третьего музыкального фрагмента вторым тестом.

Четвертый музыкальный фрагмент



Рисунок П3.7 – Распределения значений результатов тестирования младшего битового слоя четвертого музыкального фрагмента

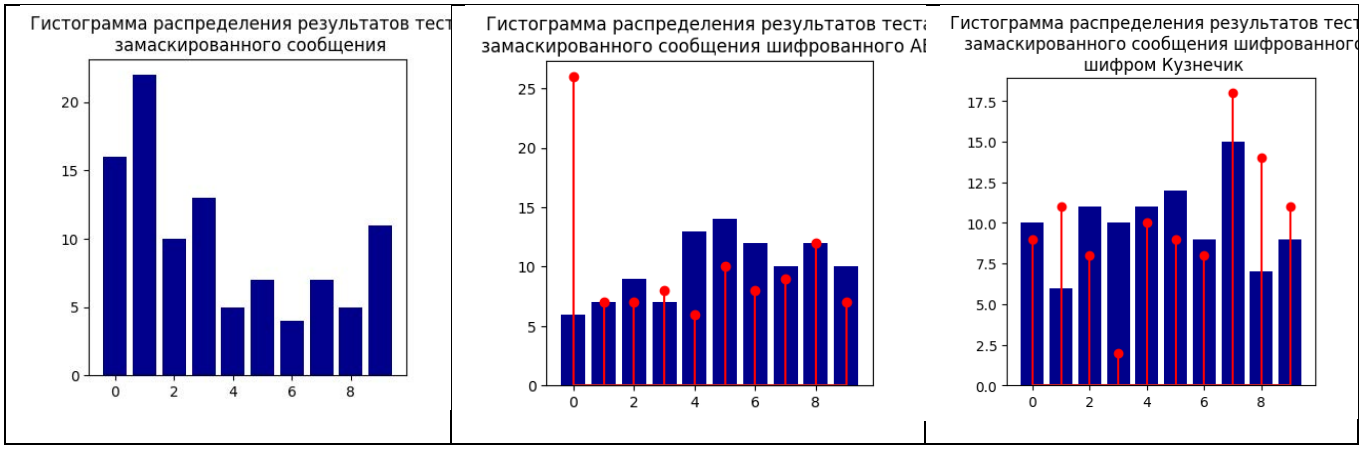


Рисунок П3.8 – Распределения значений результатов тестирования стегосистем четвертого музыкального фрагмента вторым тестом.

Результат проведения девятого теста.

Первый музыкальный фрагмент.

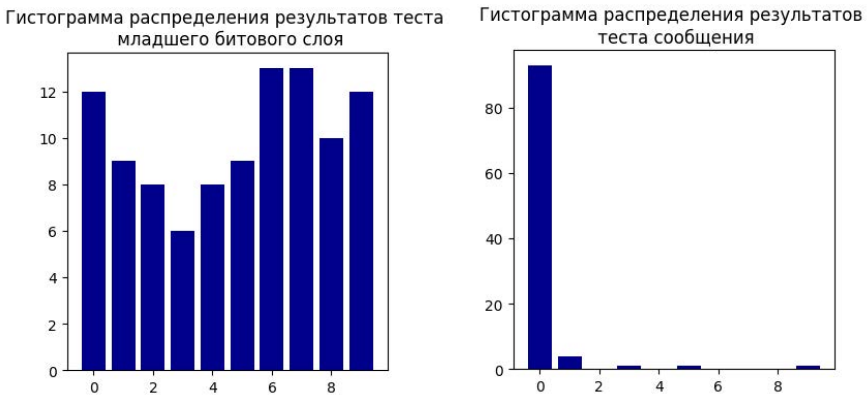


Рисунок П3.9 – Распределения значений результатов тестирования младшего битового слоя первого музыкального фрагмента и сообщения



Рисунок П3.10 – Распределения значений результатов тестирования стегосистем первого музыкального фрагмента девятым тестом.

Второй музыкальный фрагмент.



Рисунок П3.11 – Распределения значений результатов тестирования младшего битового слоя второго музыкального фрагмента

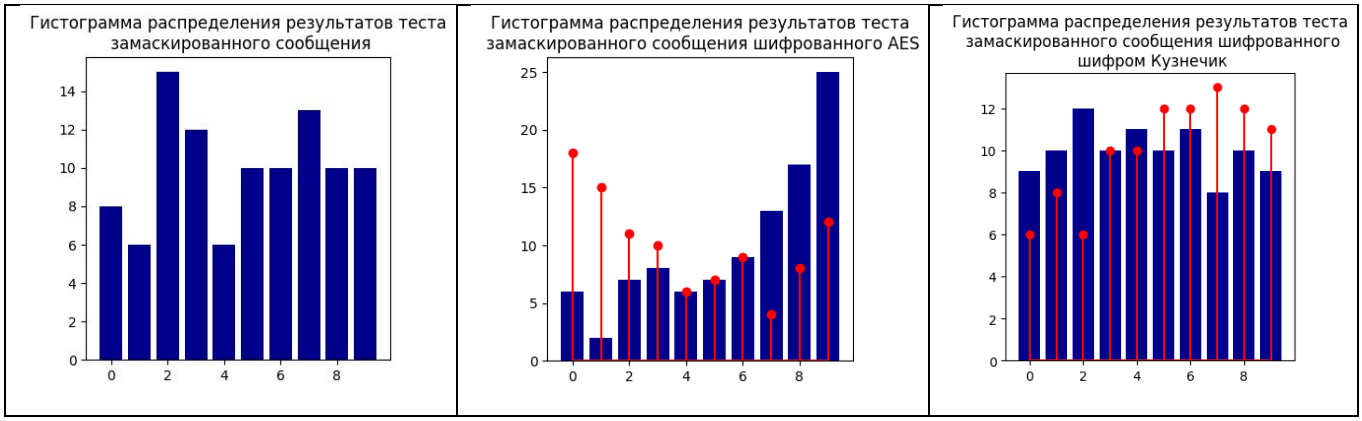


Рисунок П3.12 – Распределения значений результатов тестирования стегосистем второго музыкального фрагмента девятым тестом.

Третий музыкальный фрагмент.



Рисунок П3.13 – Распределения значений результатов тестирования младшего битового слоя третьего музыкального фрагмента

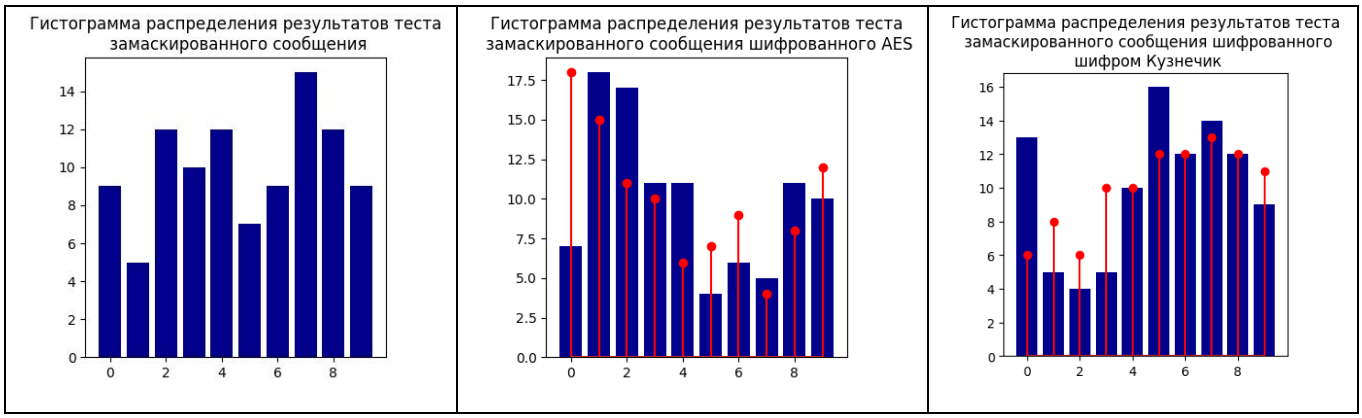


Рисунок П3.14 – Распределения значений результатов тестирования стегосистем третьего музыкального фрагмента девятым тестом.

Четвертый музыкальный фрагмент.



Рисунок П3.15 – Распределения значений результатов тестирования младшего битового слоя четвертого музыкального фрагмента

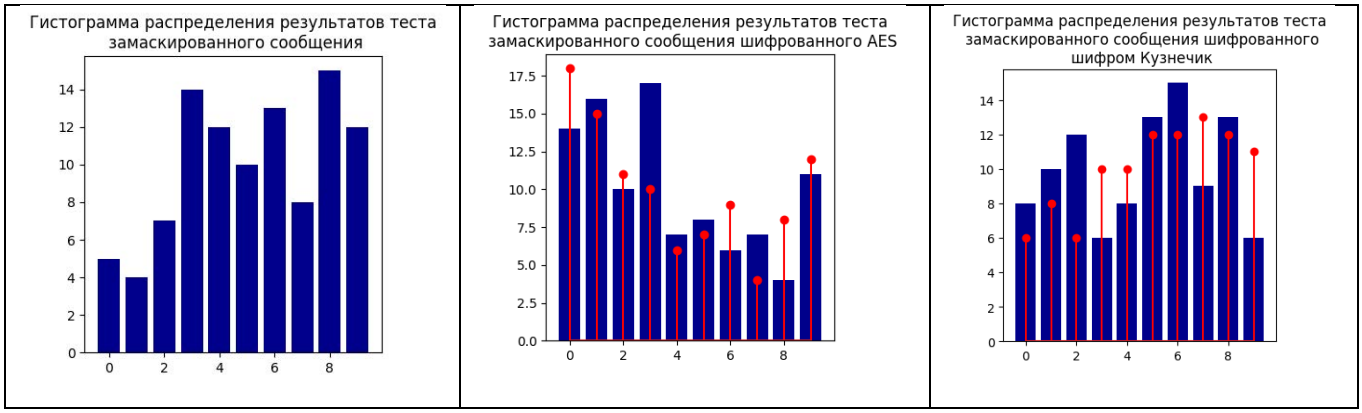


Рисунок П3.16 – Распределения значений результатов тестирования стегосистем четвертого музыкального фрагмента девятым тестом.

Результат проведения тринадцатого теста (первый вариант).

Первый музыкальный фрагмент.

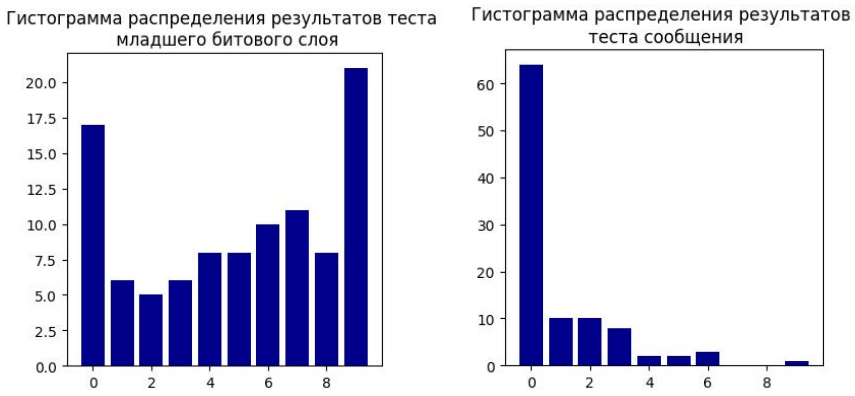


Рисунок П3.17 – Распределения значений результатов тестирования младшего битового слоя первого музыкального фрагмента и сообщения

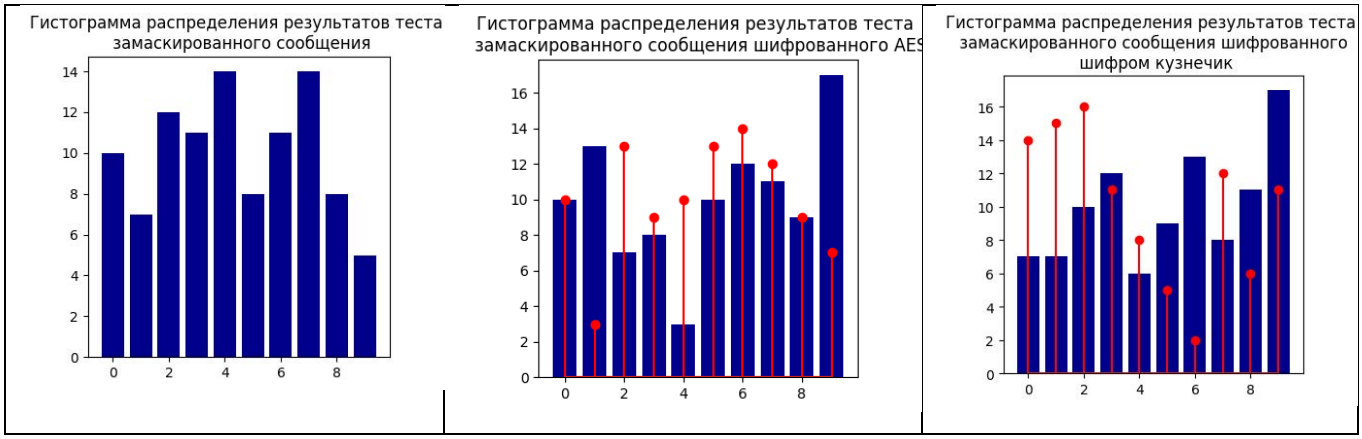


Рисунок П3.18 – Распределения значений результатов тестирования стегосистем первого музыкального фрагмента тринадцатым тестом.

Второй музыкальный фрагмент.



Рисунок П3.19 – Распределения значений результатов тестирования младшего битового слоя второго музыкального фрагмента

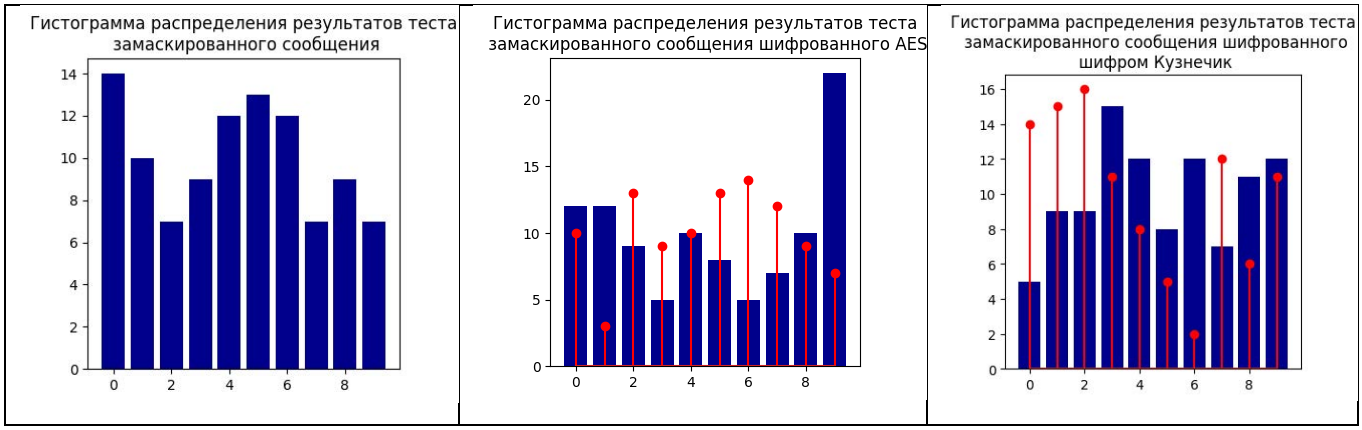


Рисунок П3.20 – Распределения значений результатов тестирования стегосистем второго музыкального фрагмента тринадцатым тестом.

Третий музыкальный фрагмент.

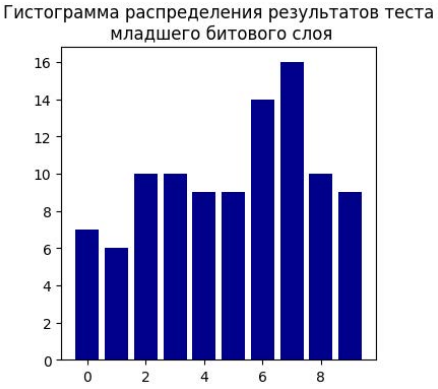


Рисунок П3.21 – Распределения значений результатов тестирования младшего битового слоя третьего музыкального фрагмента

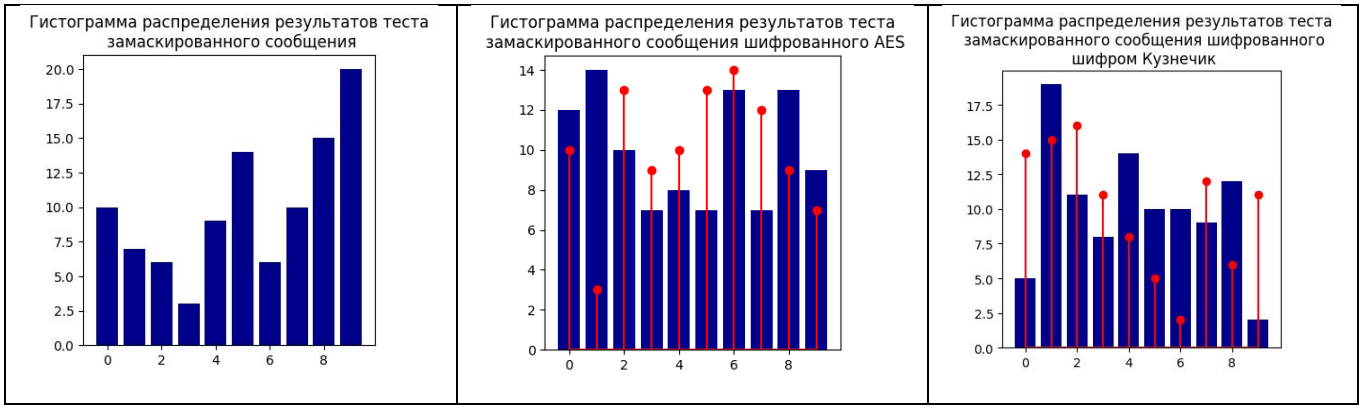


Рисунок П3.22 – Распределения значений результатов тестирования стегосистем третьего музыкального фрагмента тринадцатым тестом.

Четвертый музыкальный фрагмент.

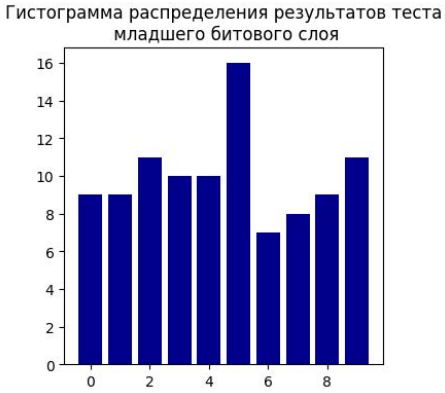


Рисунок П3.23 – Распределения значений результатов тестирования младшего битового слоя четвертого музыкального фрагмента



Рисунок П3.24 – Распределения значений результатов тестирования стегосистем четвертого музыкального фрагмента тринадцатым тестом.

Результат проведения тринадцатого теста (второй вариант).

Первый музыкальный фрагмент.

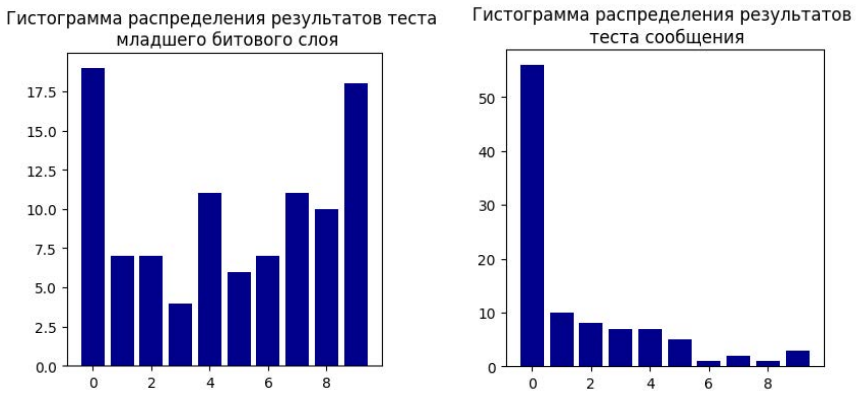


Рисунок П3.25 – Распределения значений результатов тестирования младшего битового слоя первого музыкального фрагмента и сообщения

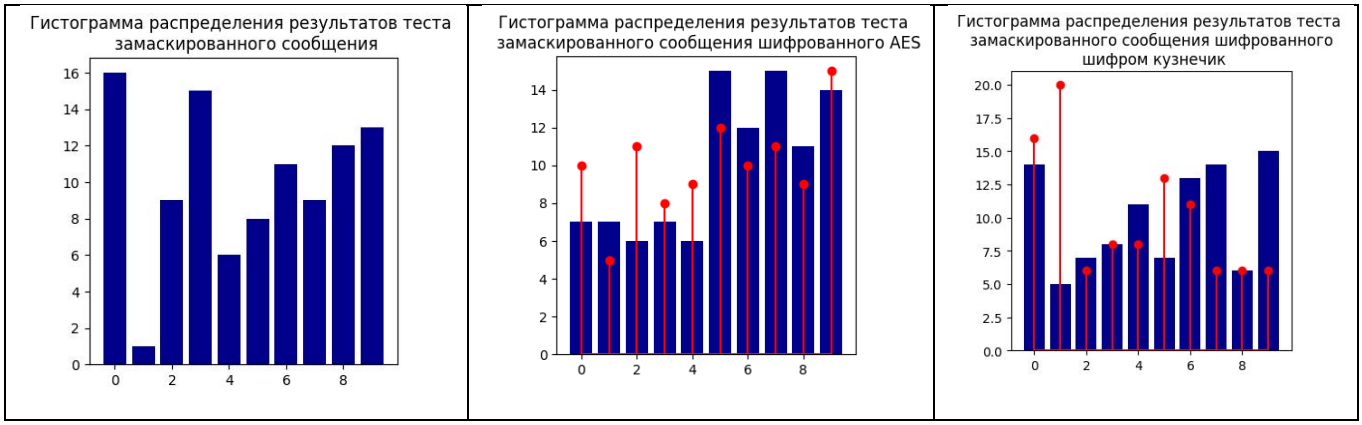


Рисунок П3.26 – Распределения значений результатов тестирования стегосистем первого музыкального фрагмента тринадцатым тестом.

Второй музыкальный фрагмент.



Рисунок П3.27 – Распределения значений результатов тестирования младшего битового слоя второго музыкального фрагмента

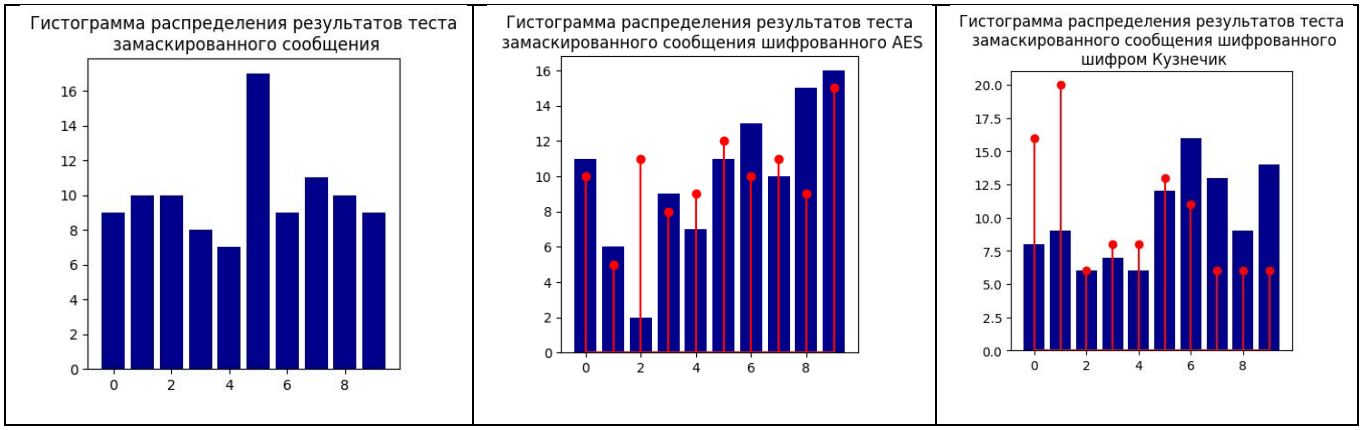


Рисунок П3.28 – Распределения значений результатов тестирования стегосистем второго музыкального фрагмента тринадцатым тестом.

Третий музыкальный фрагмент.

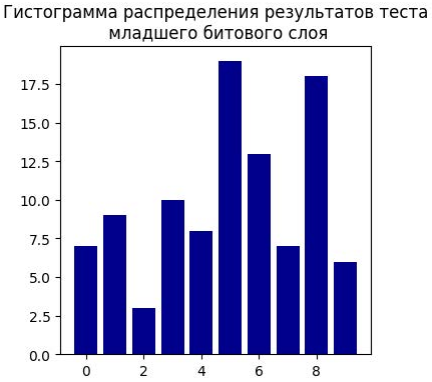


Рисунок П3.29 – Распределения значений результатов тестирования младшего битового слоя третьего музыкального фрагмента

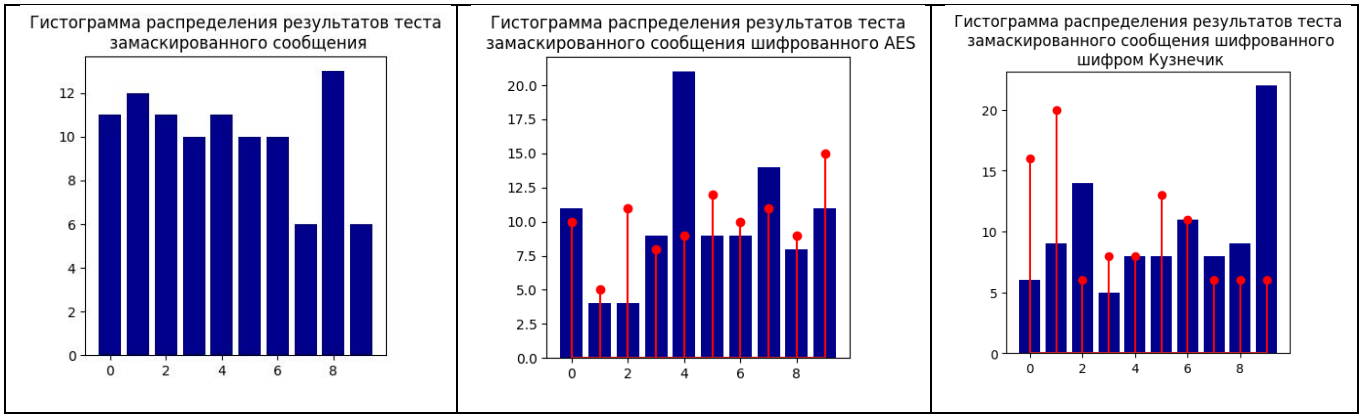


Рисунок П3.30 – Распределения значений результатов тестирования стегосистем третьего музыкального фрагмента тринадцатым тестом.

Четвертый музыкальный фрагмент.

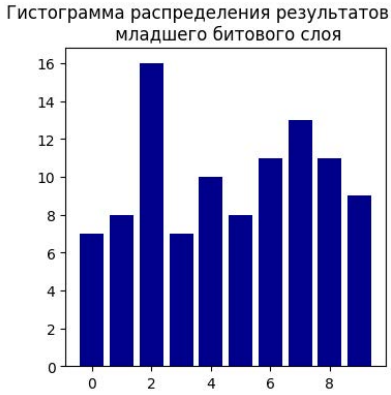


Рисунок П3.31 – Распределения значений результатов тестирования младшего битового слоя четвертого музыкального фрагмента

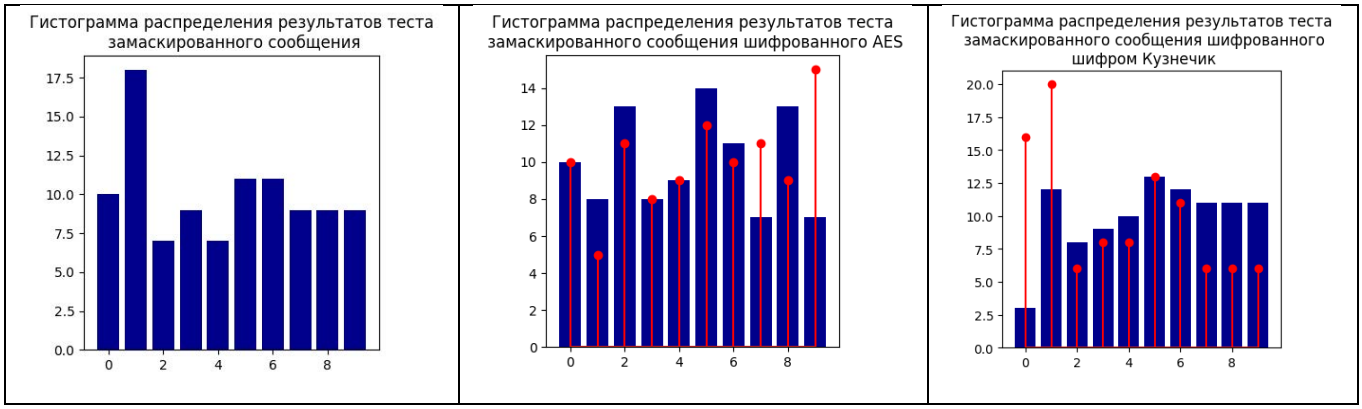


Рисунок П3.32 – Распределения значений результатов тестирования стегосистем четвертого музыкального фрагмента тринадцатым тестом.

П3.2 Тестирование музыкальных фрагментов при многослойном встраивании двух компонент в пределах одного отсчета с использованием функции исключающего ИЛИ

Фрагмент 1. Тест 1. Слой 0 (младший).

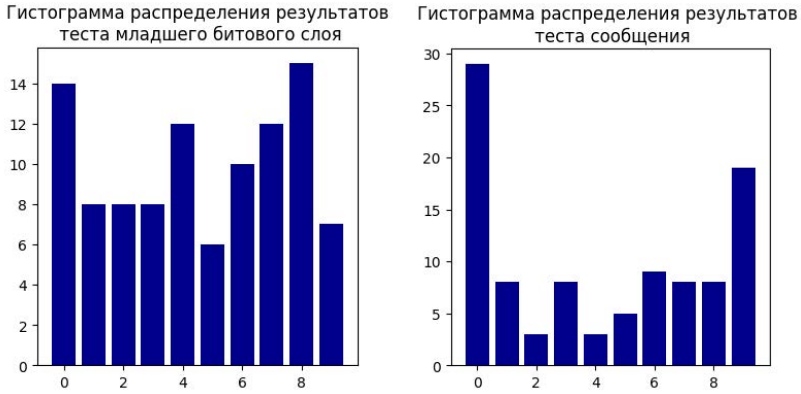


Рисунок П3.33 – Распределения значений результатов тестирования младшего битового слоя четвертого музыкального фрагмента и сообщения

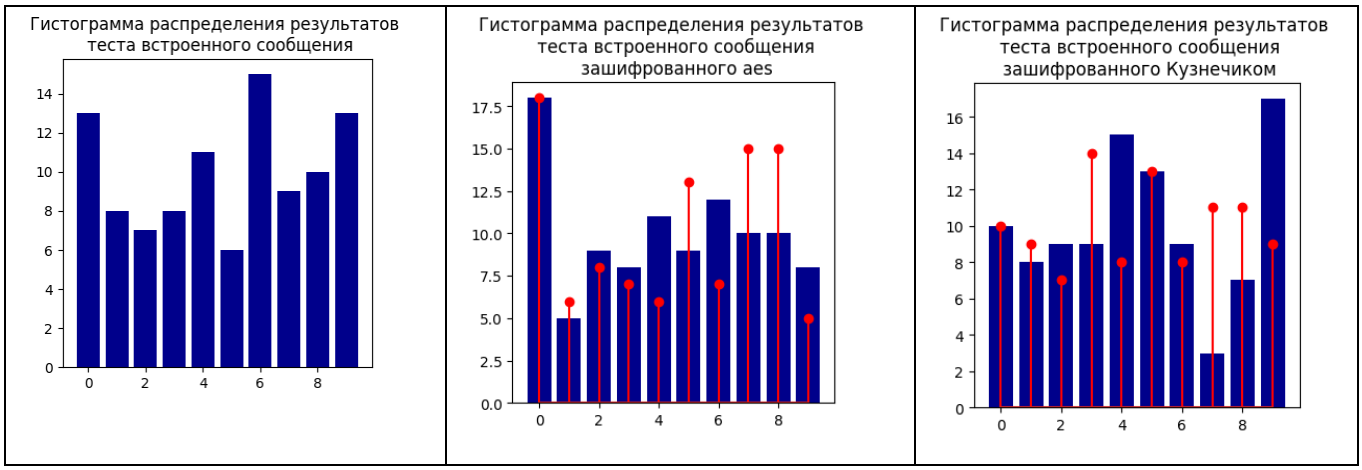


Рисунок П3.34 – Распределения значений результатов тестирования стегосистем первого музыкального фрагмента первым тестом.

Фрагмент 1. Тест 1. Слой 1.

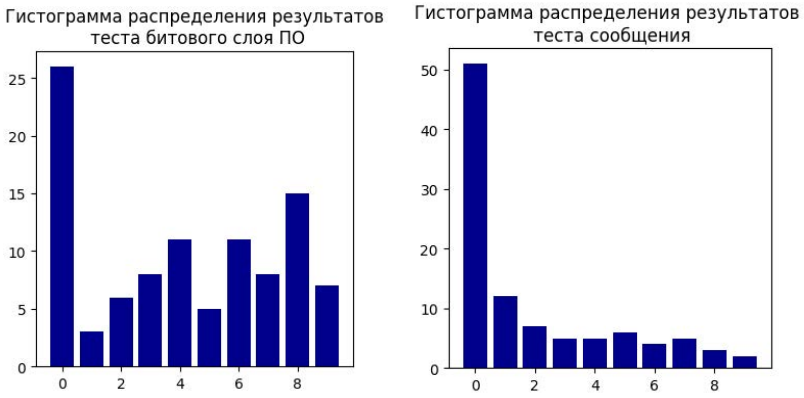


Рисунок П3.35 – Распределения значений результатов тестирования битового слоя и сообщения

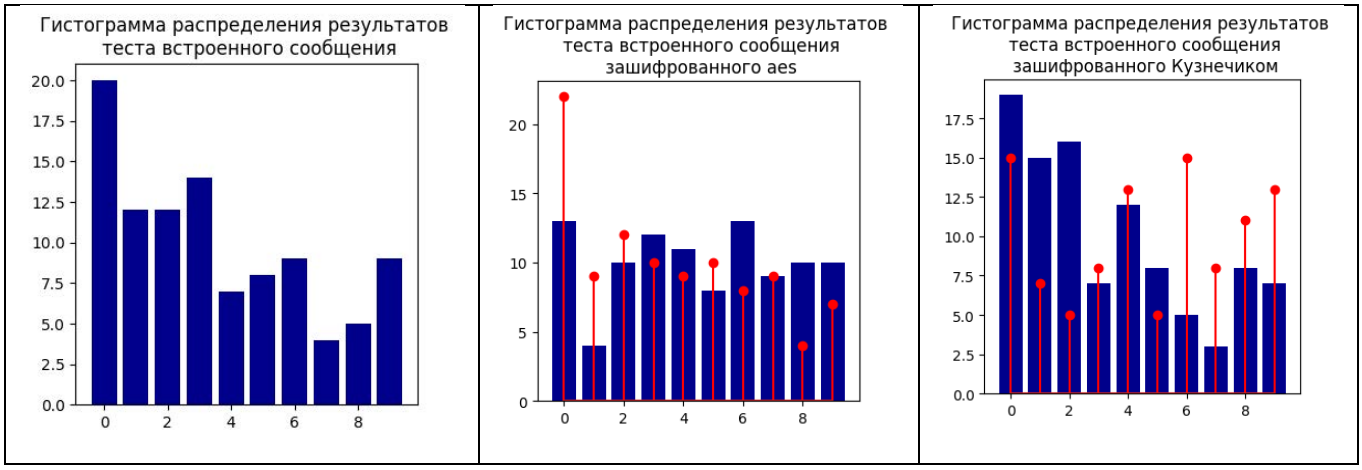


Рисунок П3.36 – Распределения значений результатов тестирования стегосистем

Фрагмент 1. Тест 1. Слой 2.

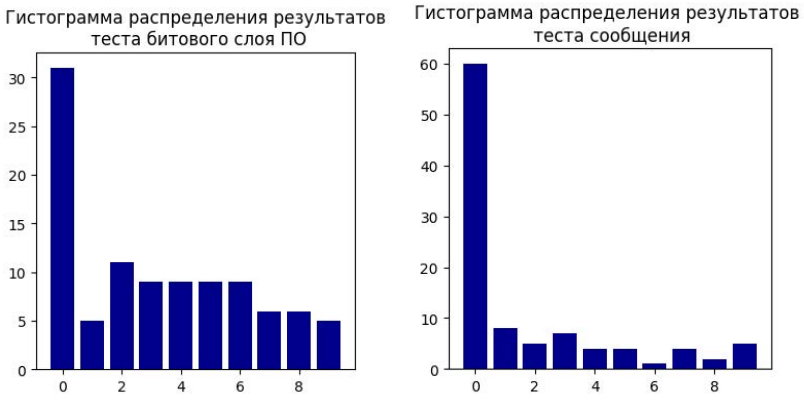


Рисунок П3.37 – Распределения значений результатов тестирования битового слоя и сообщения

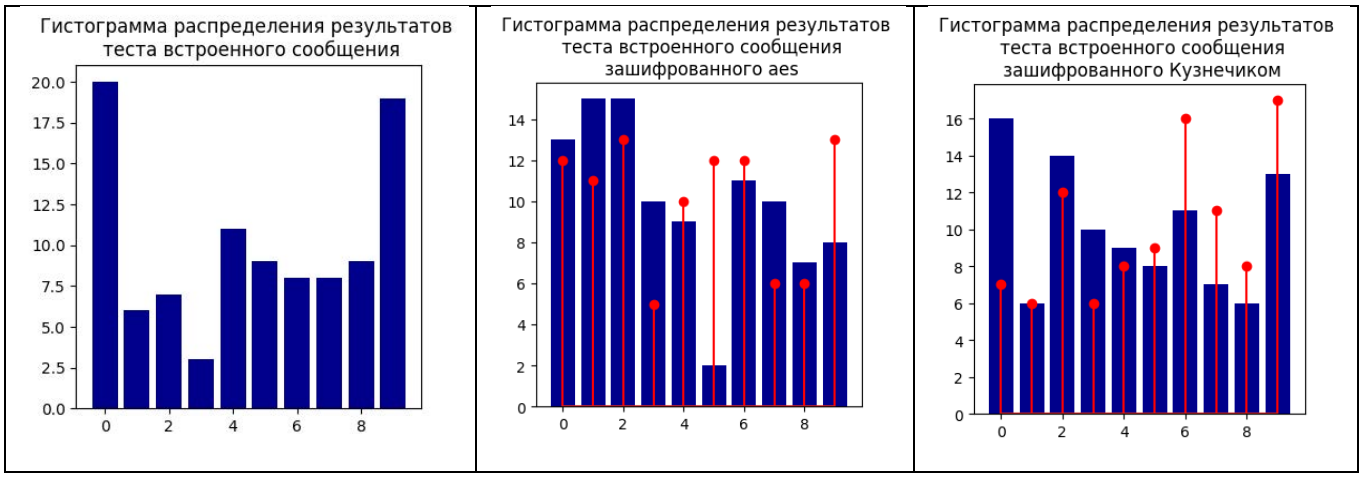


Рисунок П3.38 – Распределения значений результатов тестирования стегосистем

Фрагмент 1. Тест 1. Слой 3.

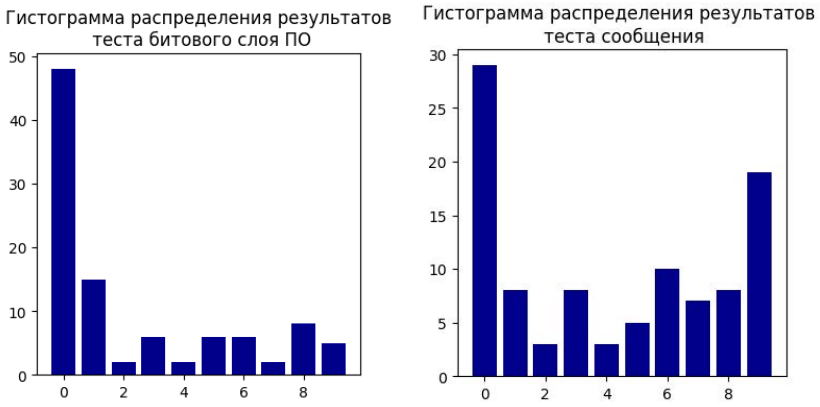


Рисунок П3.39 – Распределения значений результатов тестирования битового слоя и сообщения

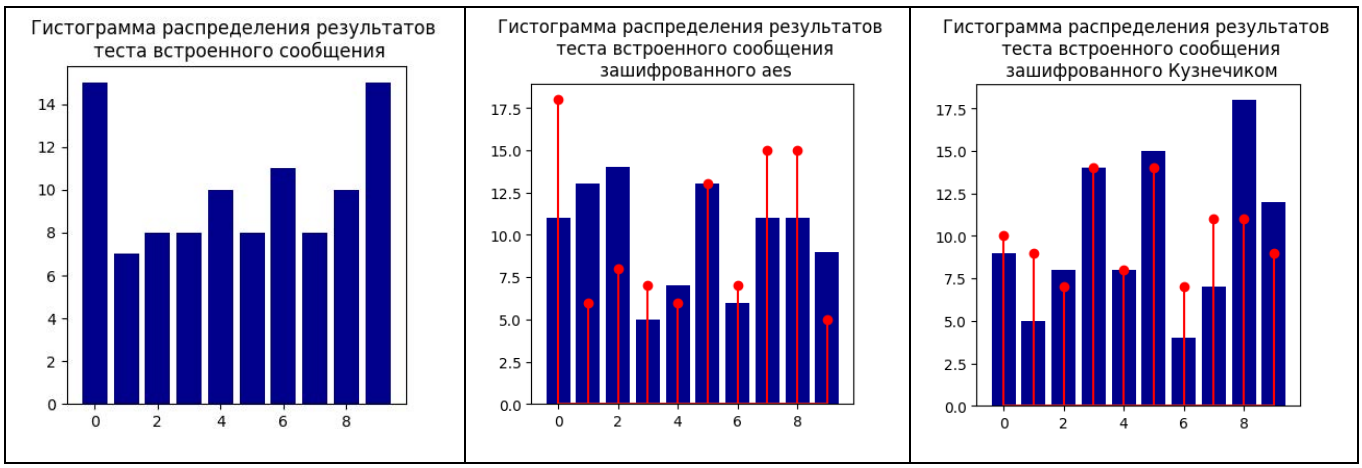


Рисунок П3.40 – Распределения значений результатов тестирования стегосистем

Фрагмент 2. Тест 1. Слой 0.

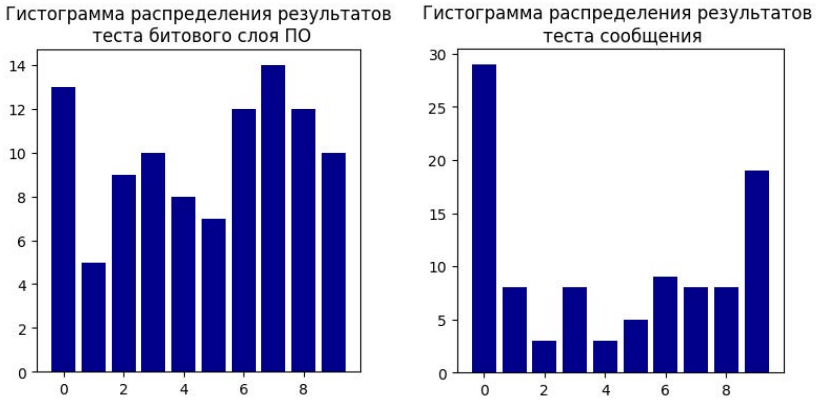


Рисунок П3.41 – Распределения значений результатов тестирования битового слоя и сообщения

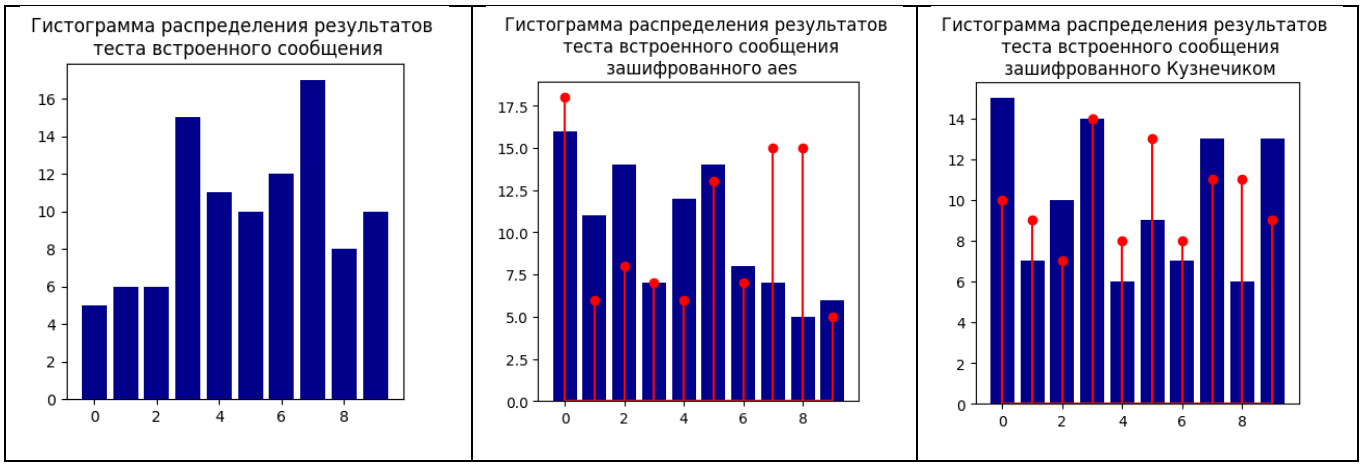


Рисунок П3.42 – Распределения значений результатов тестирования стегосистем

Фрагмент 2. Тест 1. Слой 1.

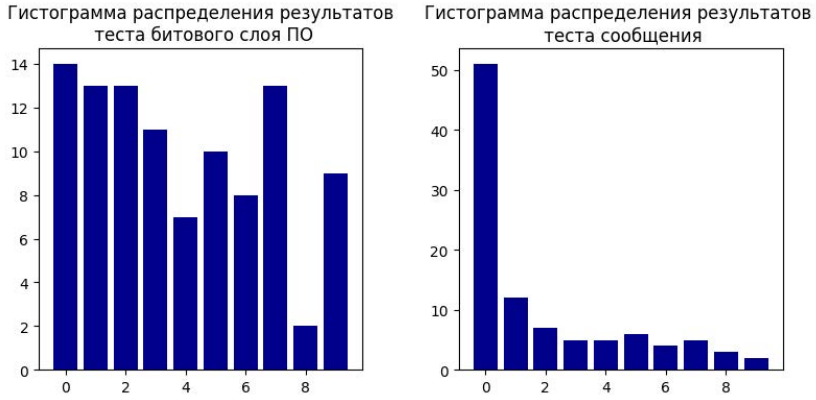


Рисунок П3.43 – Распределения значений результатов тестирования битового слоя и сообщения

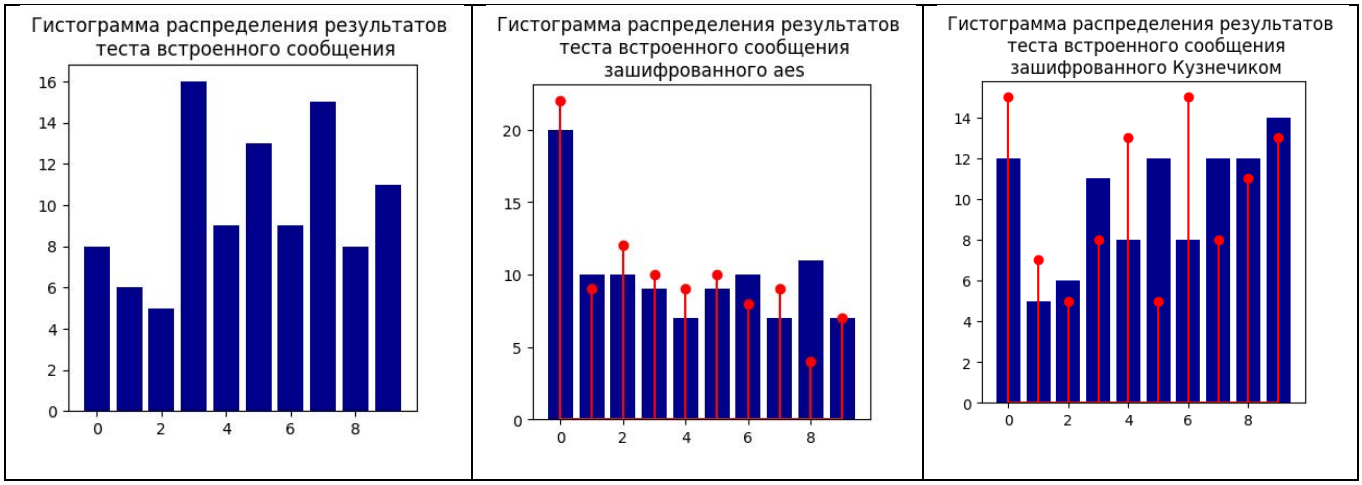


Рисунок П3.44 – Распределения значений результатов тестирования стегосистем

Фрагмент 2. Тест 1. Слой 2.

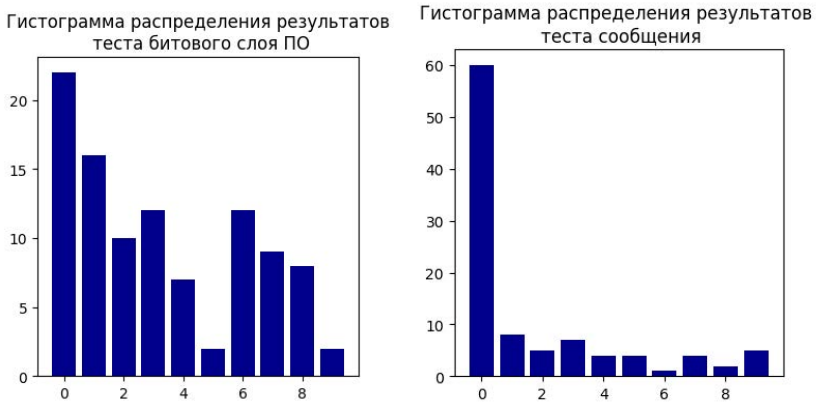


Рисунок П3.45 – Распределения значений результатов тестирования битового слоя и сообщения

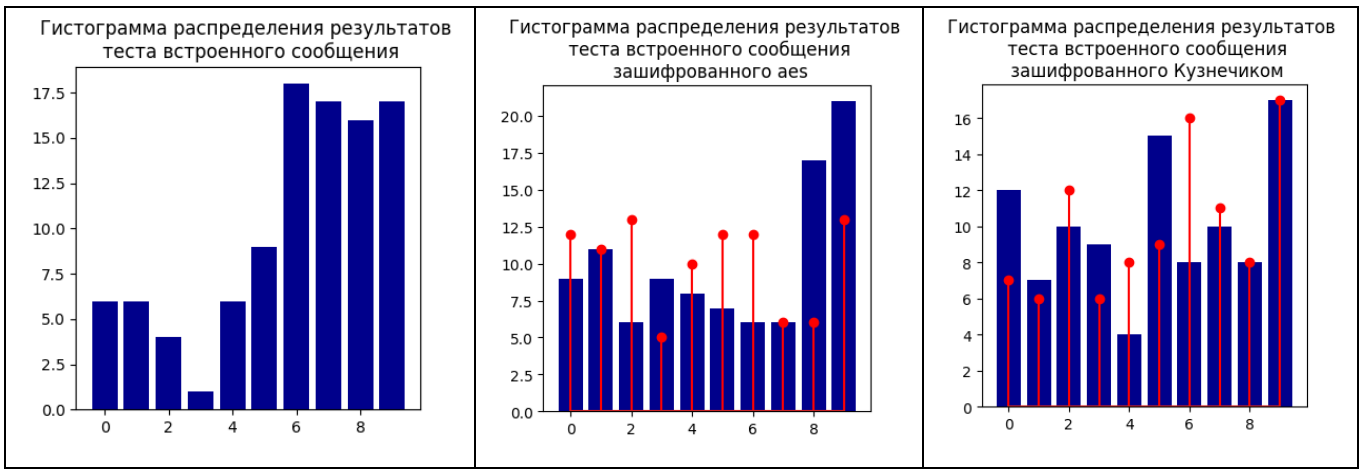


Рисунок П3.46 – Распределения значений результатов тестирования стегосистем

Фрагмент 2. Тест 1. Слой 3.

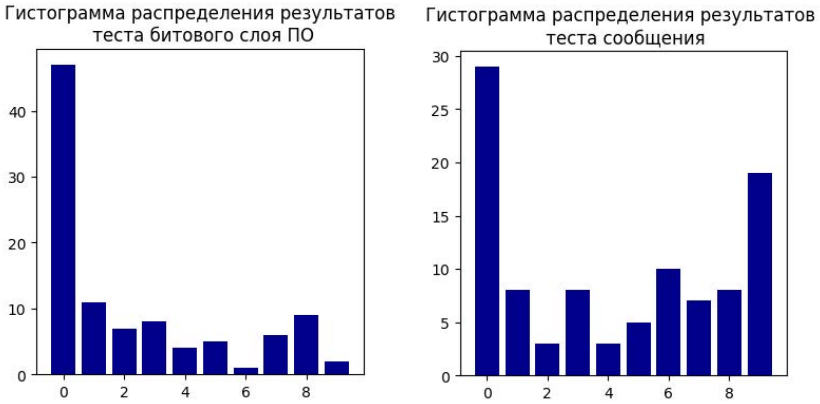


Рисунок П3.47 – Распределения значений результатов тестирования битового слоя и сообщения

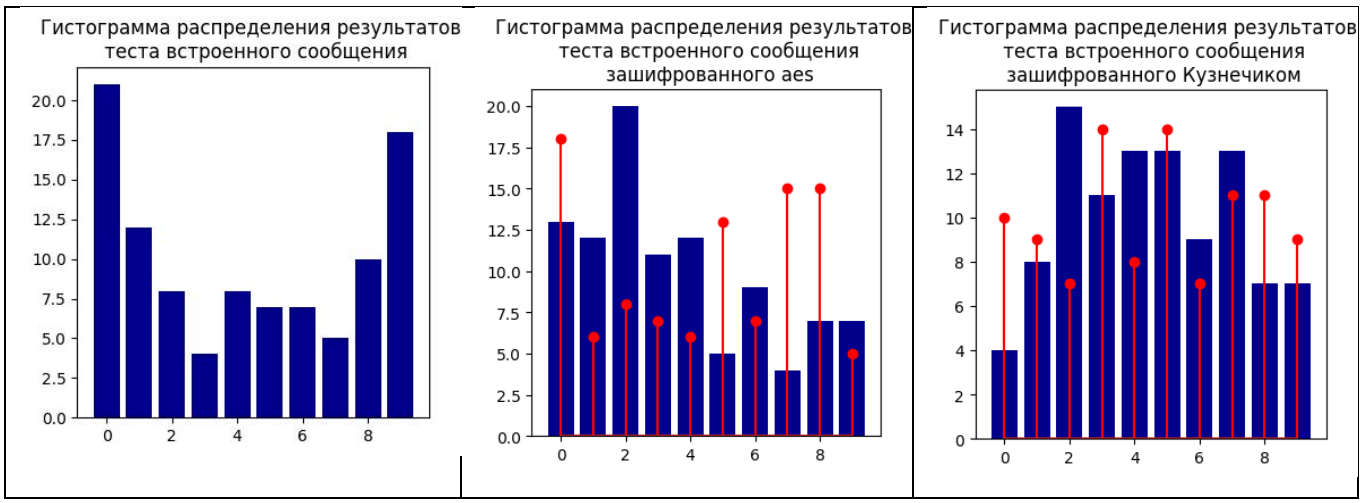


Рисунок П3.48 – Распределения значений результатов тестирования стегосистем

Фрагмент 3. Тест 1. Слой 0.

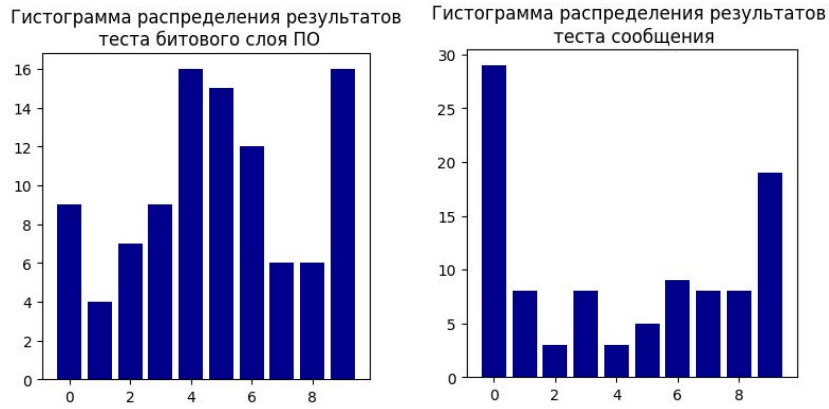


Рисунок П3.49 – Распределения значений результатов тестирования битового слоя и сообщения

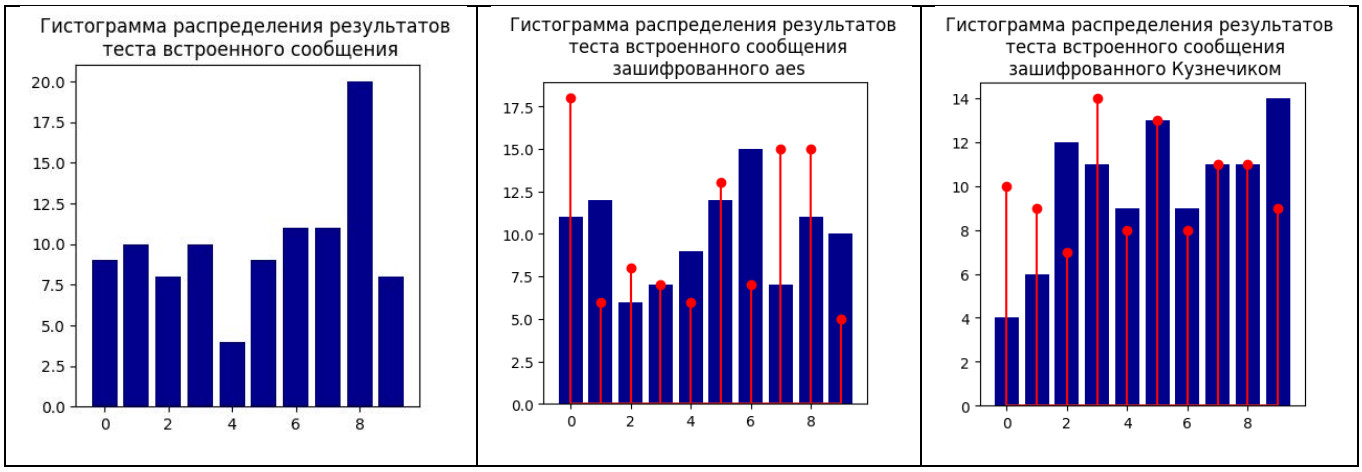


Рисунок П3.50 – Распределения значений результатов тестирования стегосистем

Фрагмент 3. Тест 1. Слой 1.

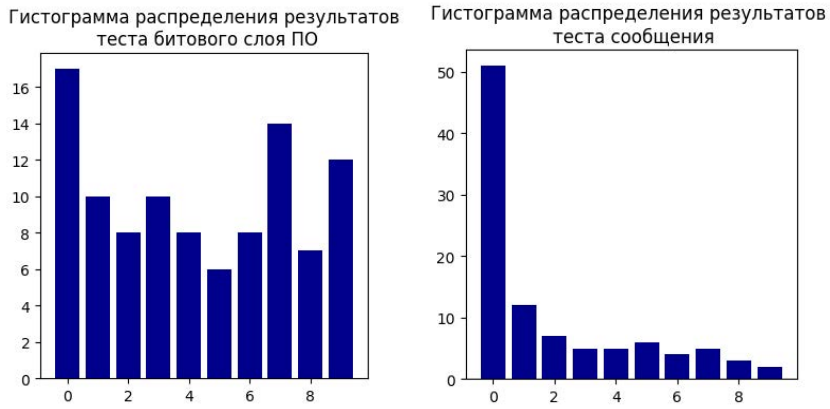


Рисунок П3.51 – Распределения значений результатов тестирования битового слоя и сообщения

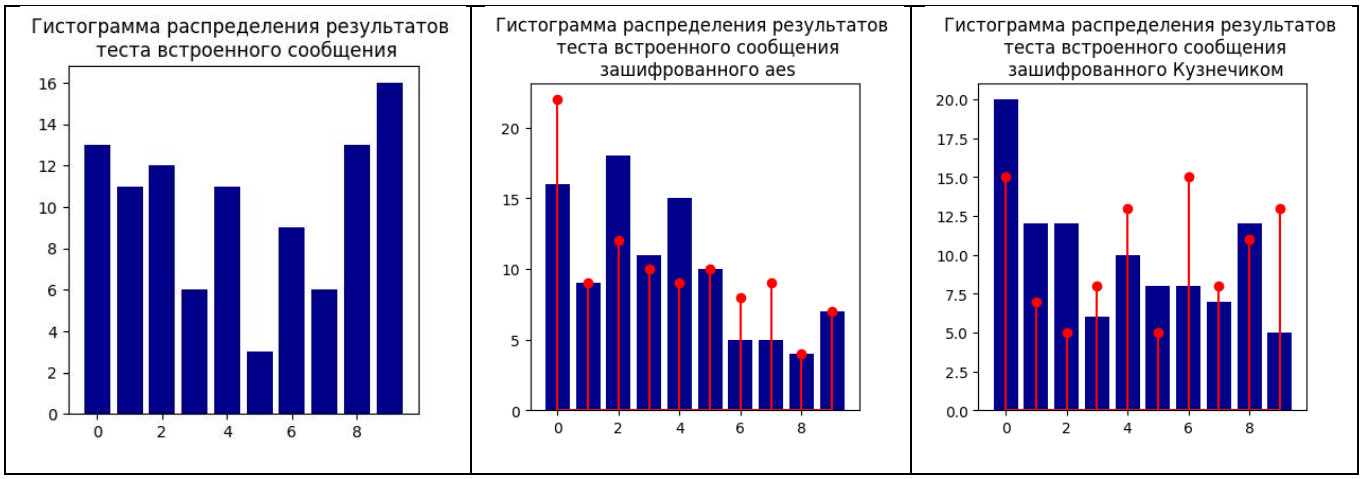


Рисунок П3.52 – Распределения значений результатов тестирования стегосистем

Фрагмент 3. Тест 1. Слой 2.

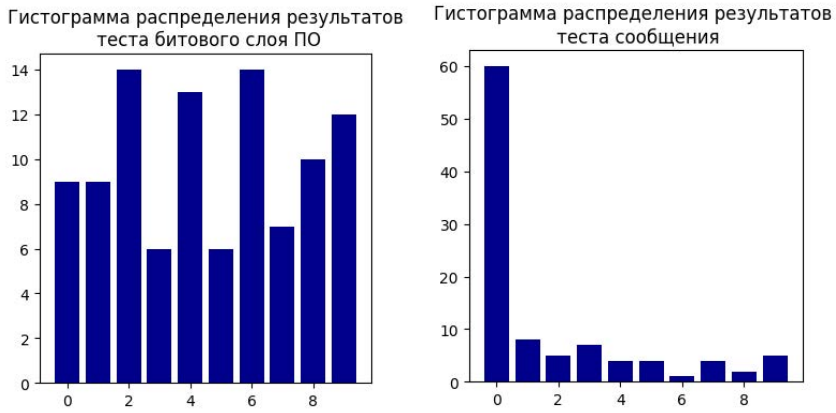


Рисунок П3.53 – Распределения значений результатов тестирования битового слоя и сообщения

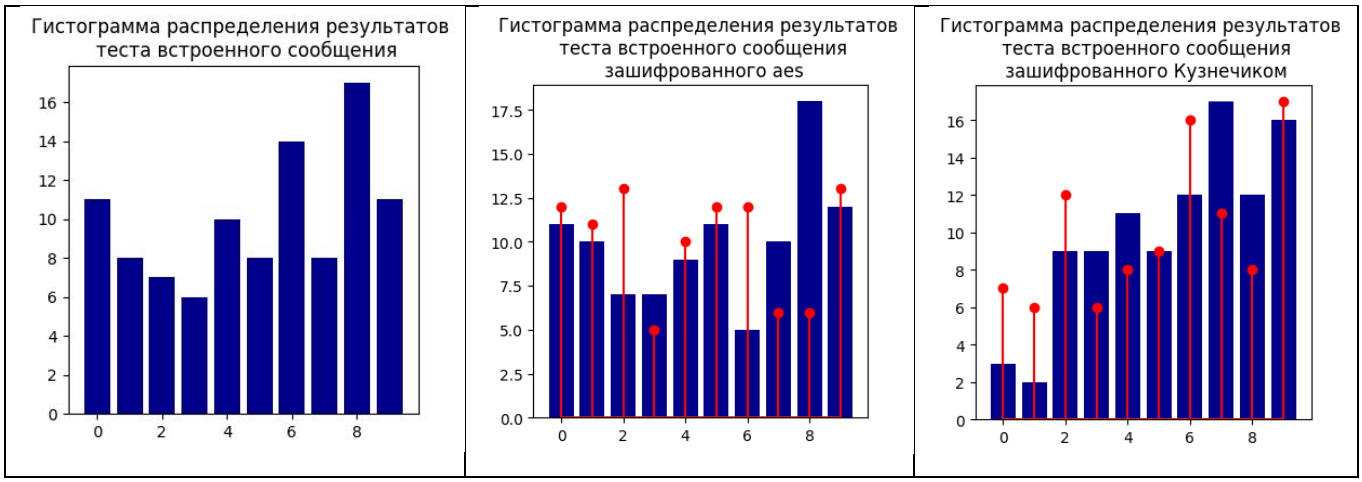


Рисунок П3.54 – Распределения значений результатов тестирования стегосистем

Фрагмент 3. Тест 1. Слой 3.

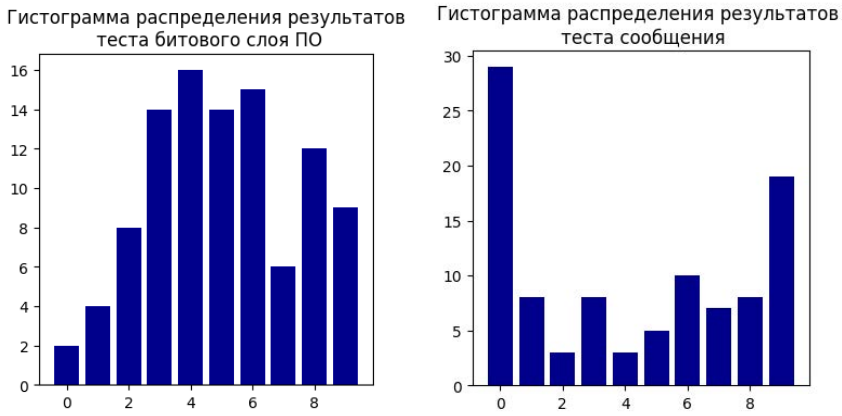


Рисунок П3.55 – Распределения значений результатов тестирования битового слоя и сообщения

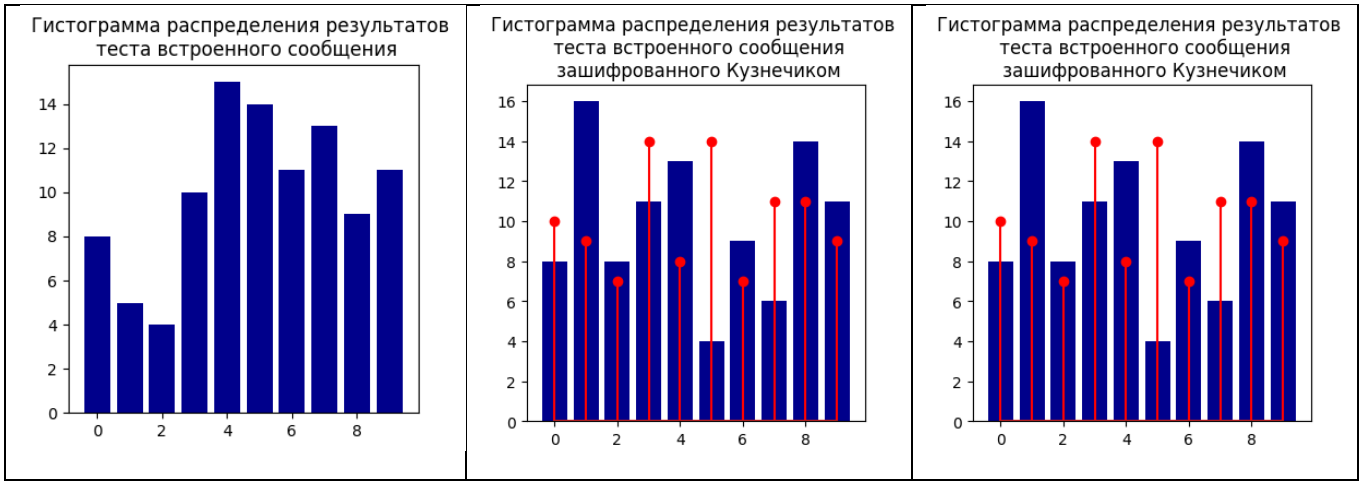


Рисунок П3.56 – Распределения значений результатов тестирования стегосистем

Фрагмент 4. Тест 1. Слой 0.

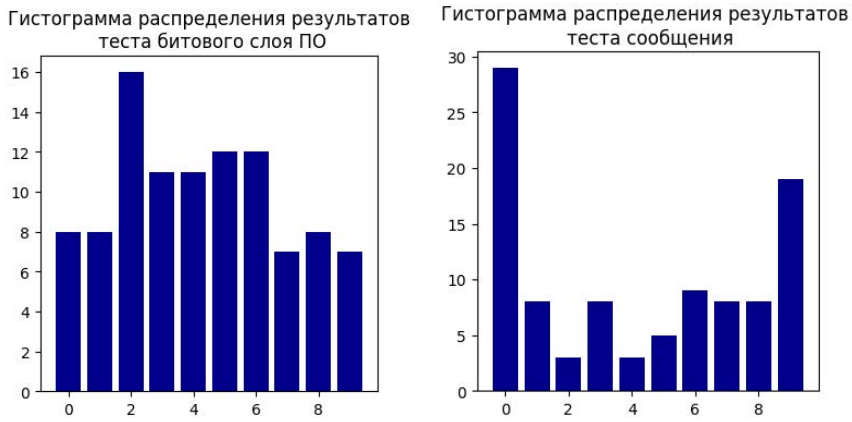


Рисунок П3.57 – Распределения значений результатов тестирования битового слоя и сообщения

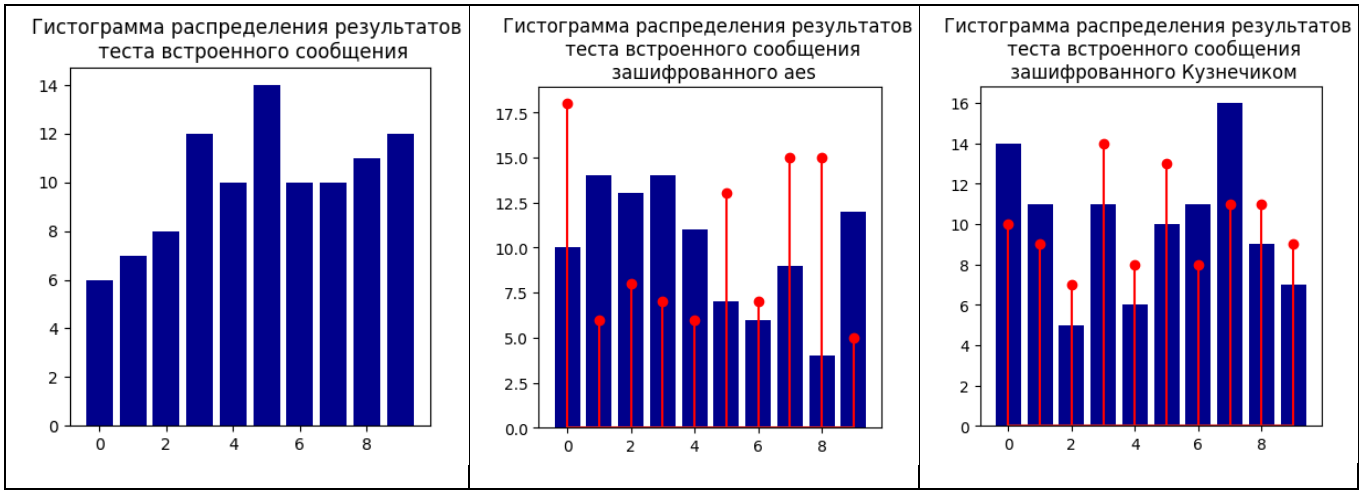


Рисунок П3.58 – Распределения значений результатов тестирования стегосистем

Фрагмент 4. Тест 1. Слой 1.

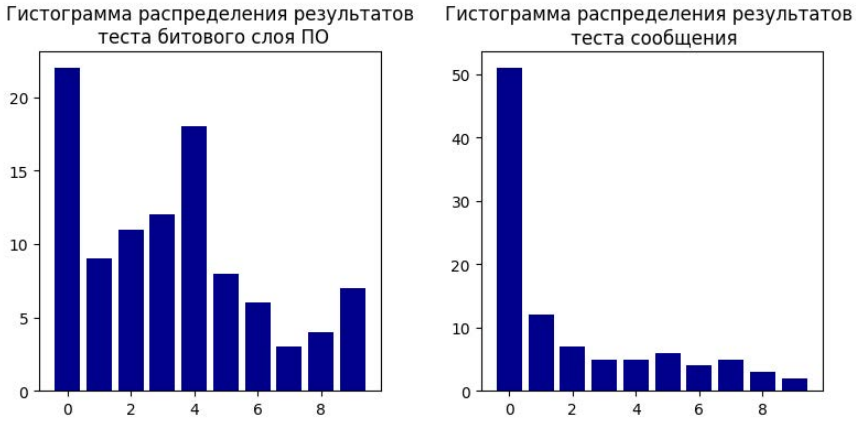


Рисунок П3.59 – Распределения значений результатов тестирования битового слоя и сообщения

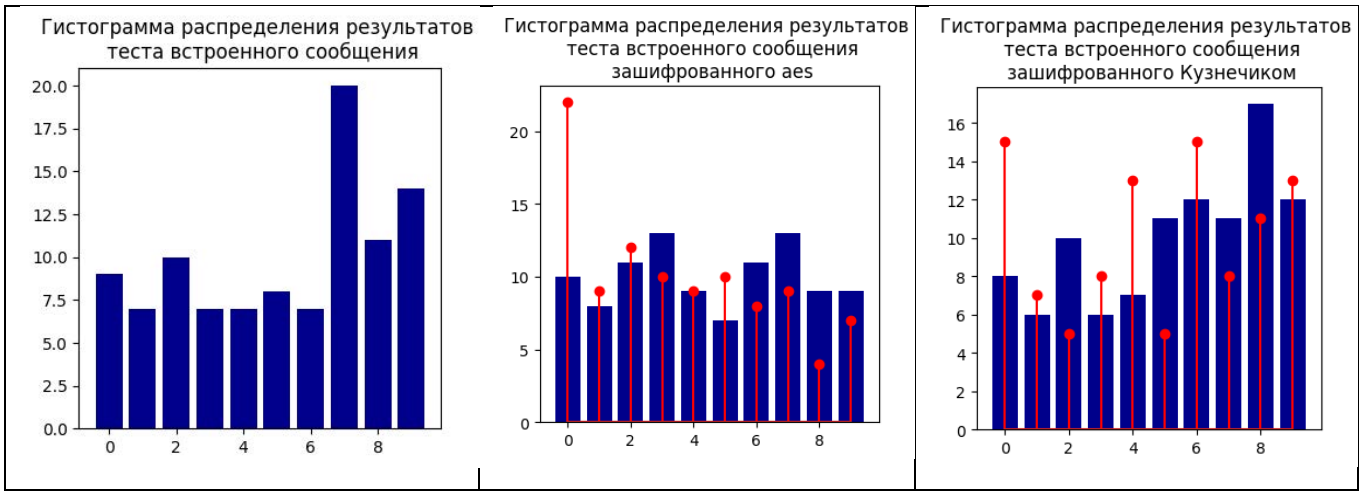


Рисунок П3.60 – Распределения значений результатов тестирования стегосистем

Фрагмент 4. Тест 1. Слой 2.

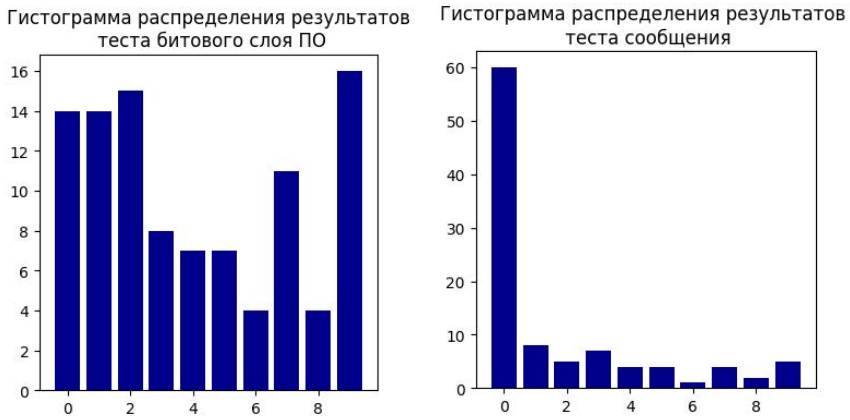


Рисунок П3.61 – Распределения значений результатов тестирования битового слоя и сообщения

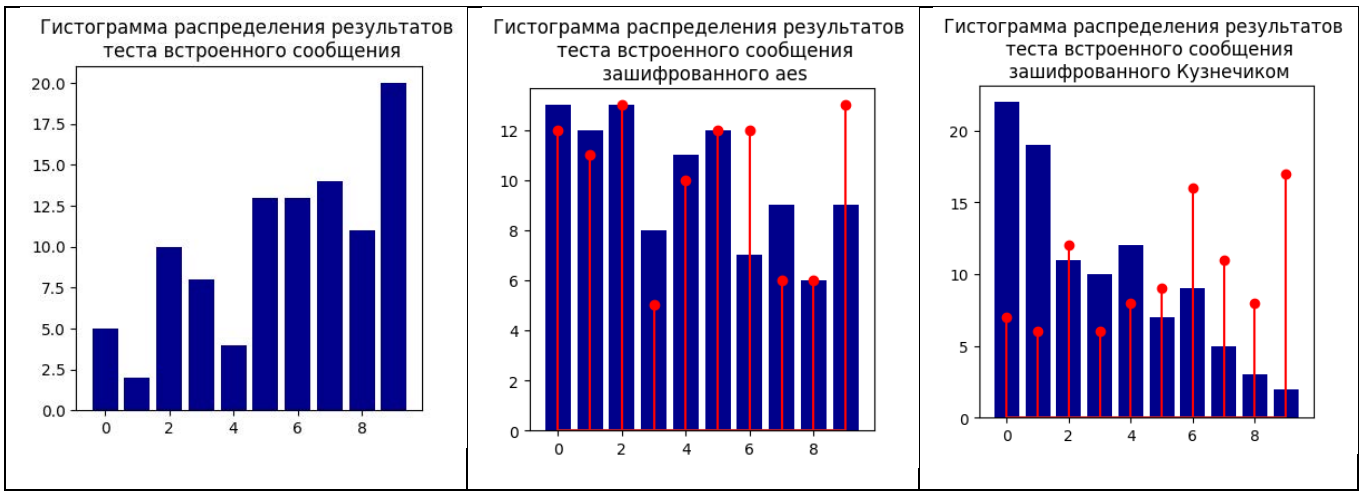


Рисунок П3.62 – Распределения значений результатов тестирования стегосистем

Фрагмент 4. Тест 1. Слой 3.

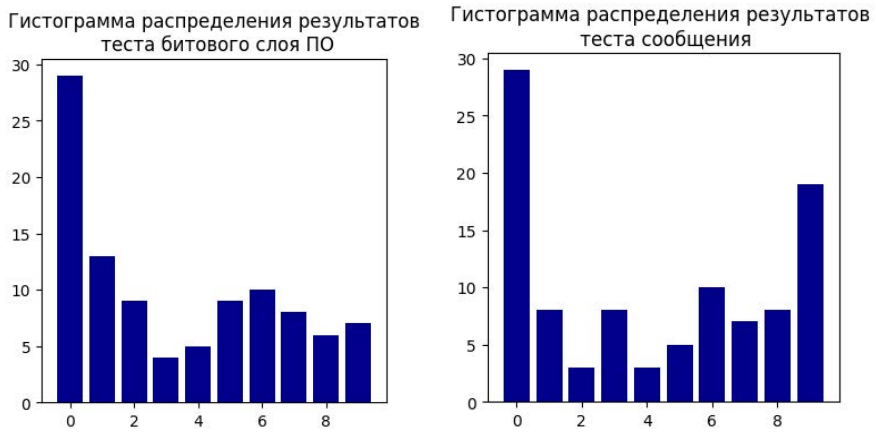


Рисунок П3.63 – Распределения значений результатов тестирования битового слоя и сообщения

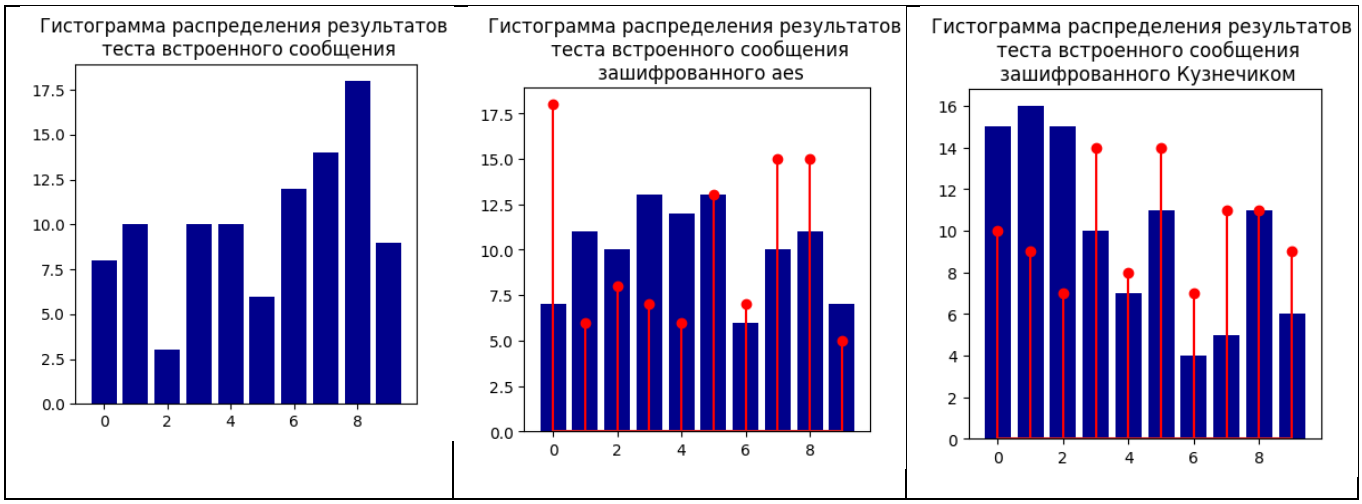


Рисунок П3.64 – Распределения значений результатов тестирования стегосистем

Фрагмент 1. Тест 12. Слой 0.

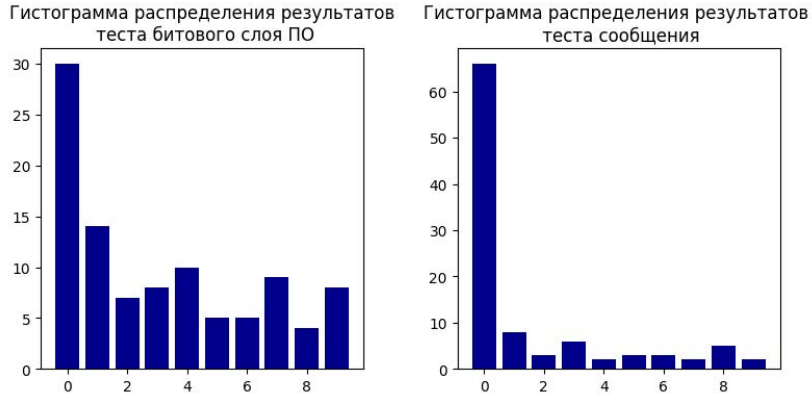


Рисунок П3.65 – Распределения значений результатов тестирования младшего битового слоя четвертого музыкального фрагмента и сообщения

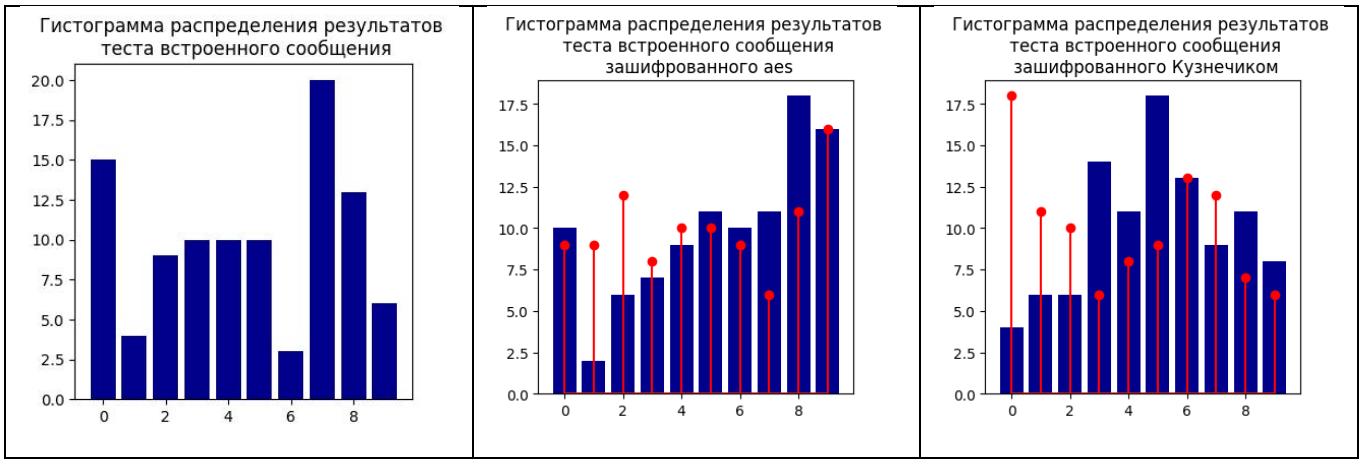


Рисунок П3.66 – Распределения значений результатов тестирования стегосистем первого музыкального фрагмента первым тестом.

Фрагмент 1. Тест 12. Слой 1.

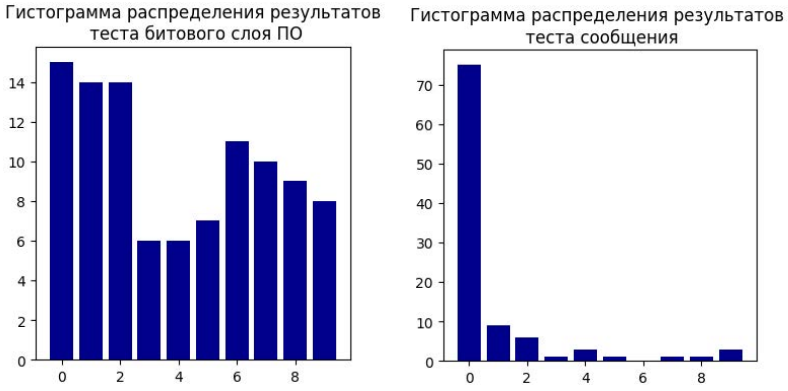


Рисунок П3.67 – Распределения значений результатов тестирования битового слоя и сообщения

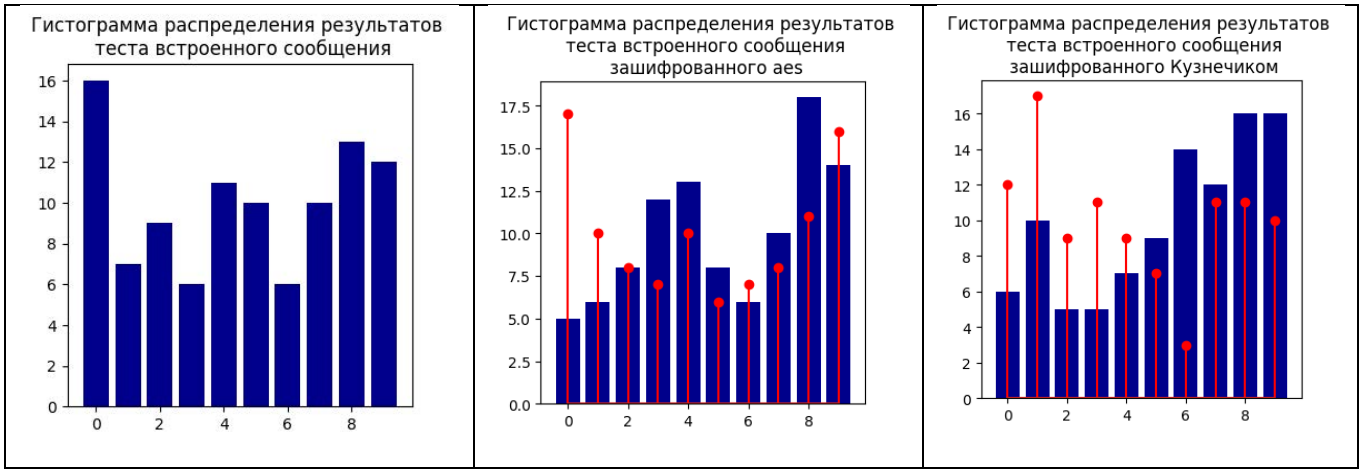


Рисунок П3.68 – Распределения значений результатов тестирования стегосистем

Фрагмент 1. Тест 12. Слой 2.

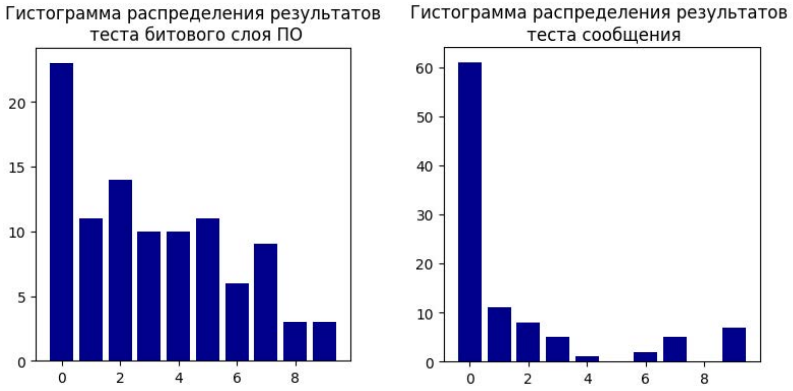


Рисунок П3.69 – Распределения значений результатов тестирования битового слоя и сообщения

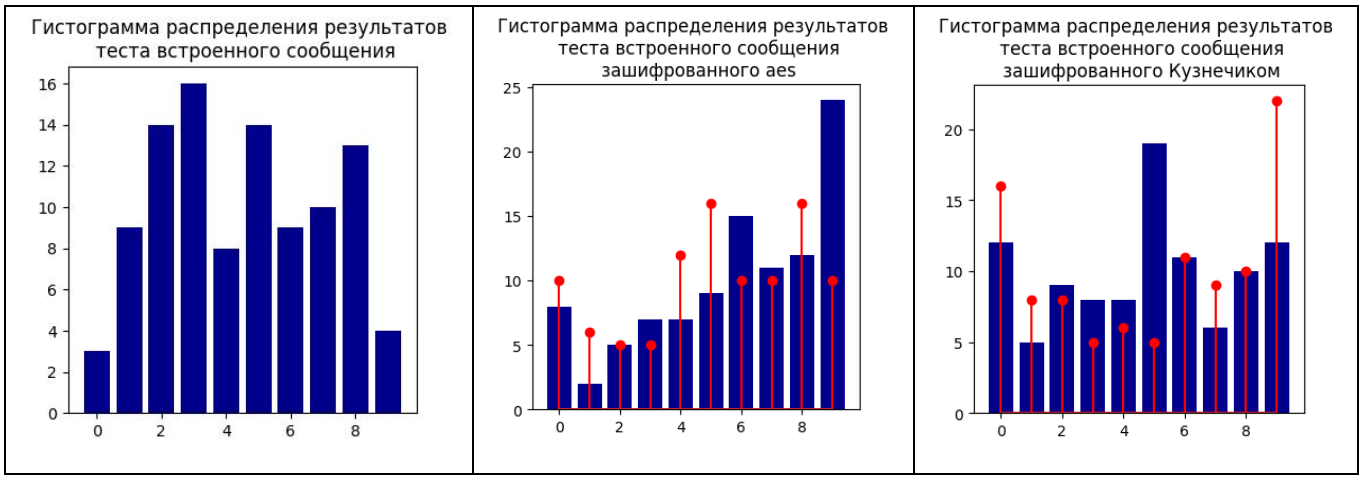


Рисунок П3.70 – Распределения значений результатов тестирования стегосистем

Фрагмент 1. Тест 12. Слой 3.

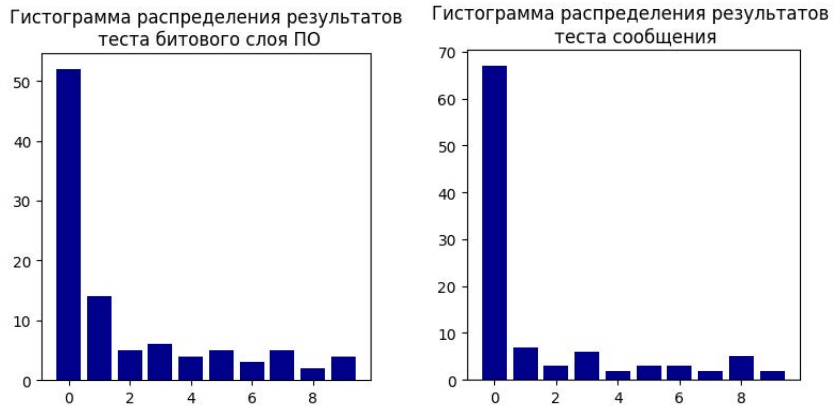


Рисунок П3.71 – Распределения значений результатов тестирования битового слоя и сообщения

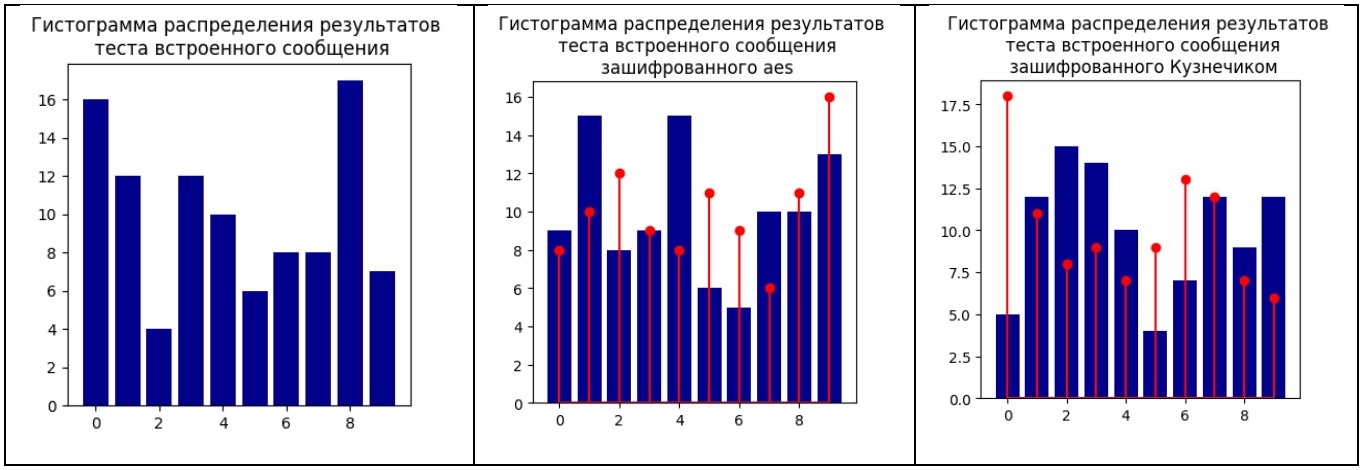


Рисунок П3.72 – Распределения значений результатов тестирования стегосистем

Фрагмент 2. Тест 12. Слой 0.

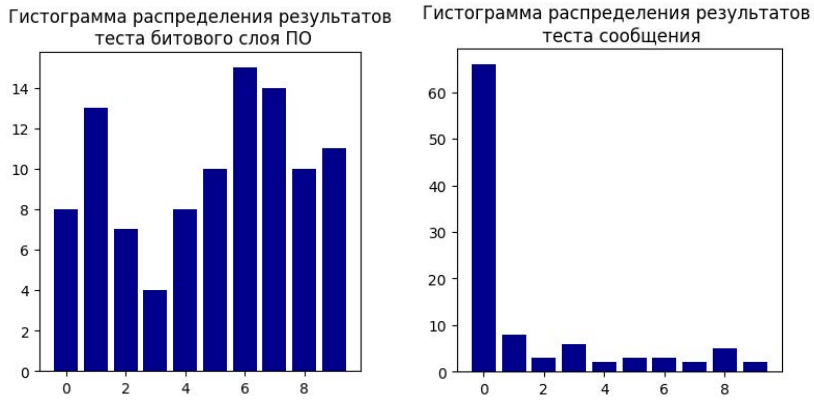


Рисунок П3.73 – Распределения значений результатов тестирования битового слоя и сообщения

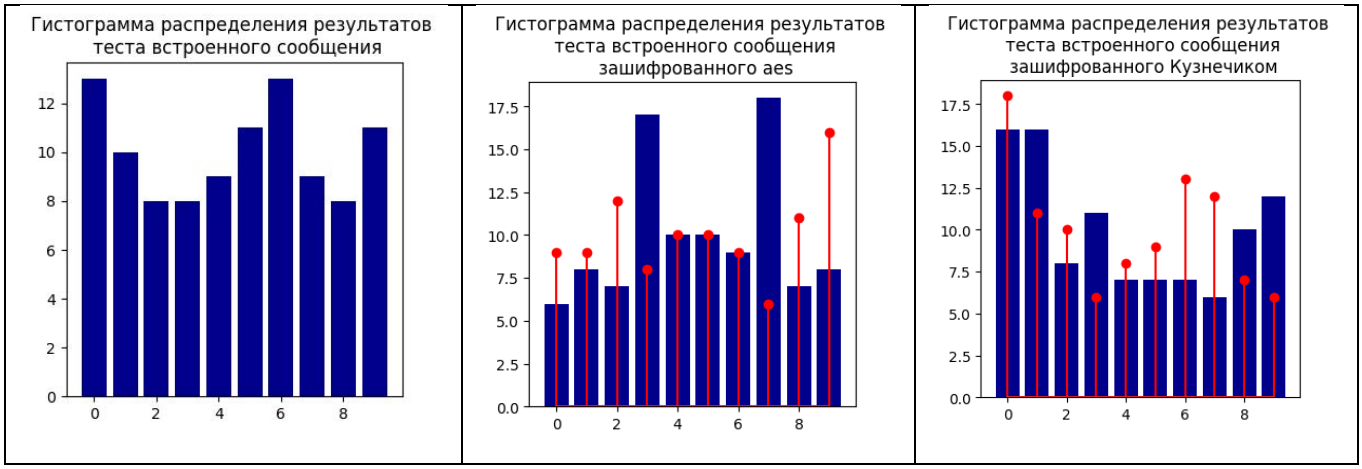


Рисунок П3.74 – Распределения значений результатов тестирования стегосистем

Фрагмент 2. Тест 1. Слой 1.

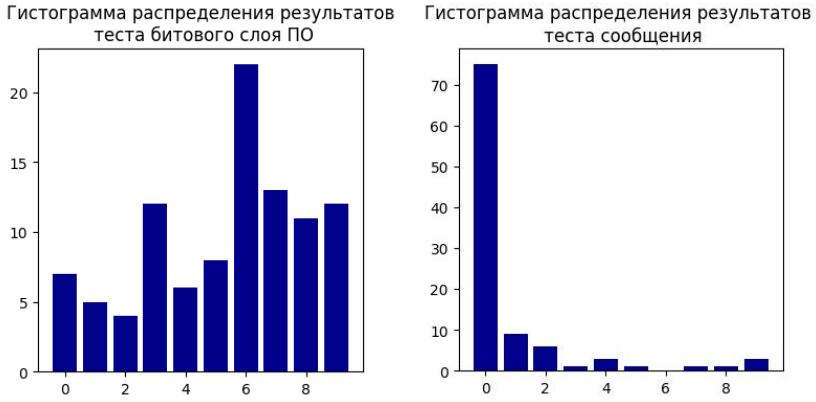


Рисунок П3.75 – Распределения значений результатов тестирования битового слоя и сообщения

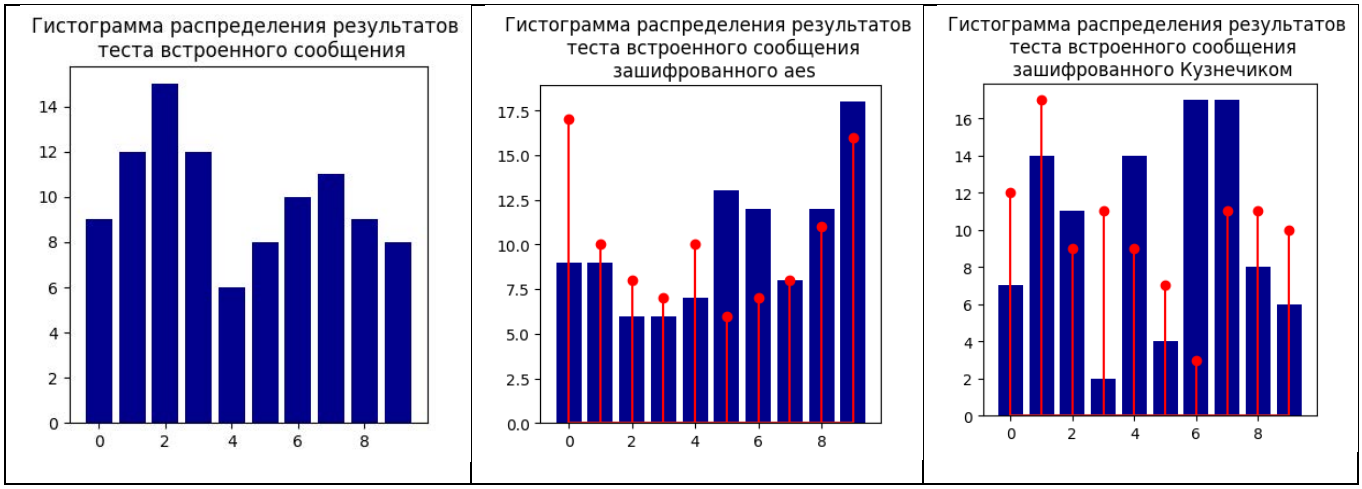


Рисунок П3.76 – Распределения значений результатов тестирования стегосистем

Фрагмент 2. Тест 12. Слой 2.

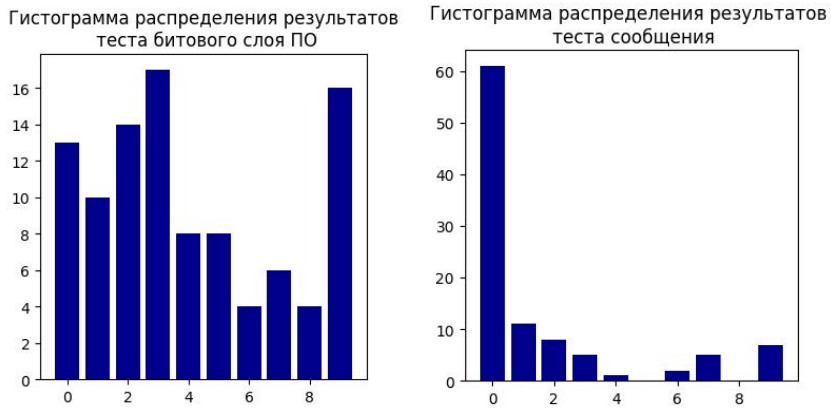


Рисунок П3.77 – Распределения значений результатов тестирования битового слоя и сообщения

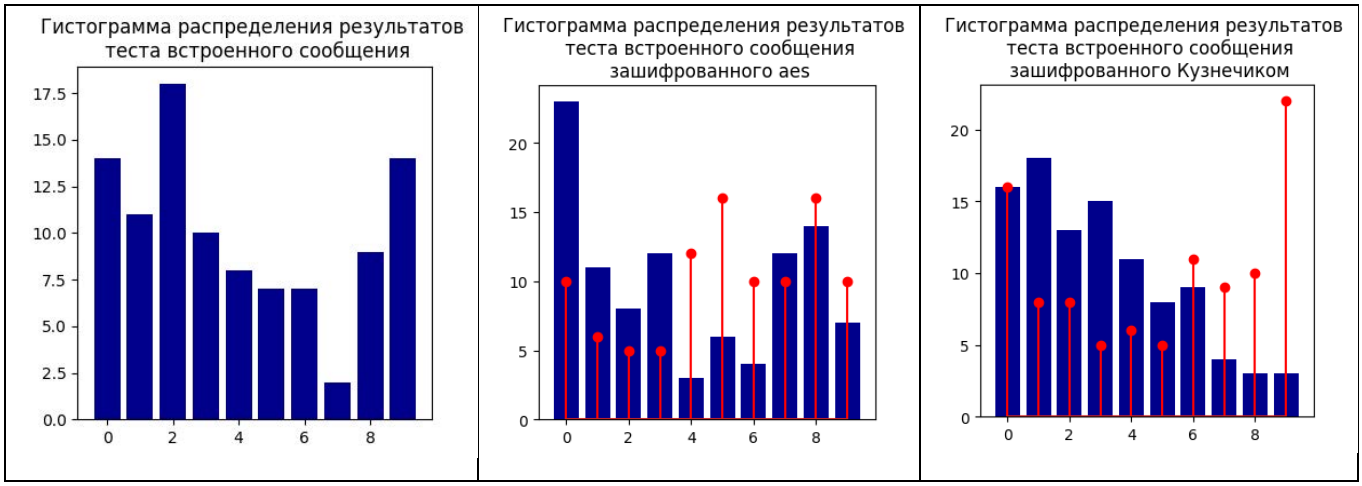


Рисунок П3.78 – Распределения значений результатов тестирования стегосистем

Фрагмент 2. Тест 12. Слой 3.

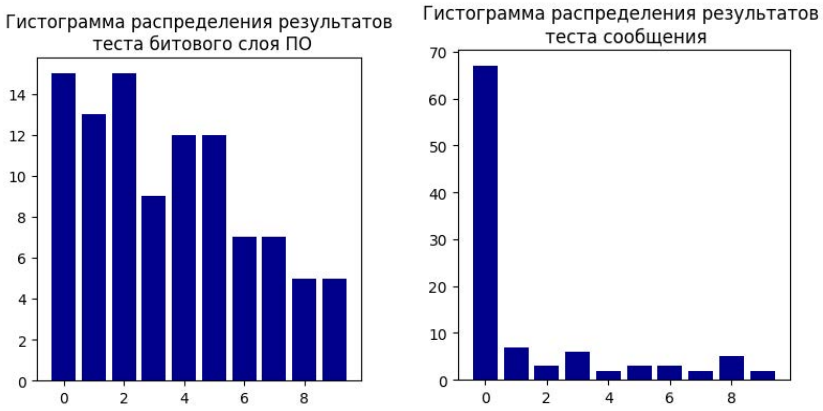


Рисунок П3.79 – Распределения значений результатов тестирования битового слоя и сообщения

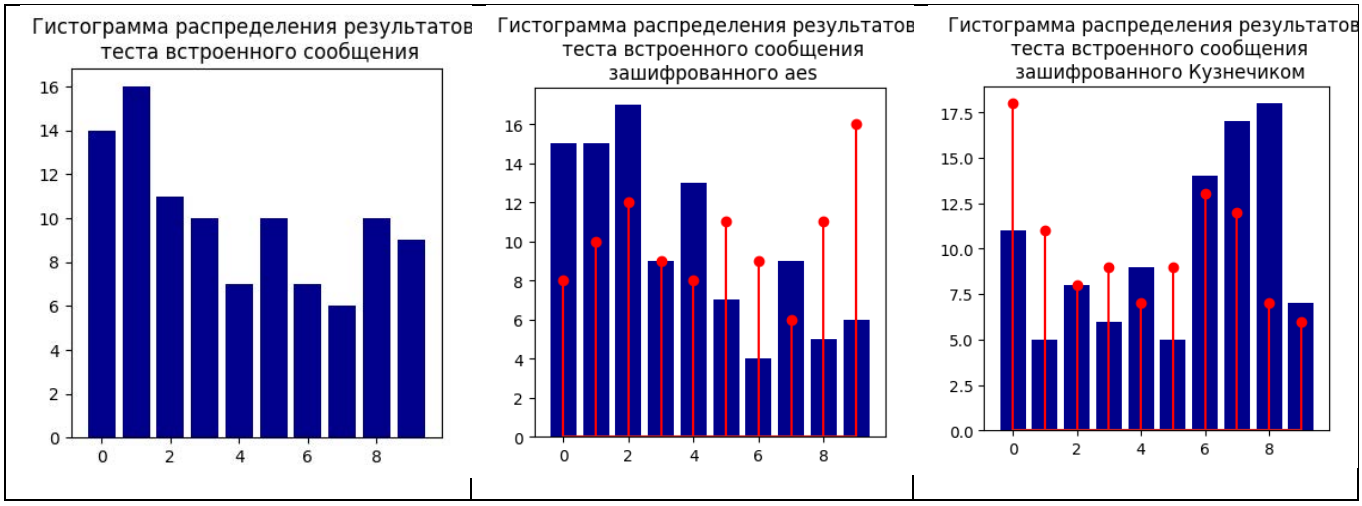


Рисунок П3.80 – Распределения значений результатов тестирования стегосистем

Фрагмент 3. Тест 1. Слой 0.

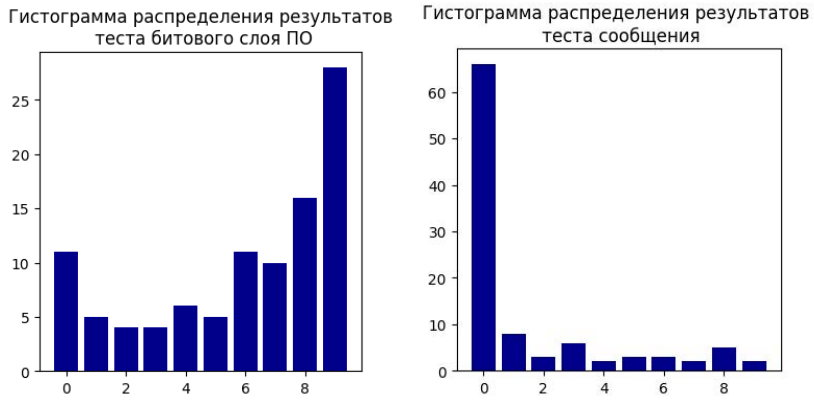


Рисунок П3.81 – Распределения значений результатов тестирования битового слоя и сообщения

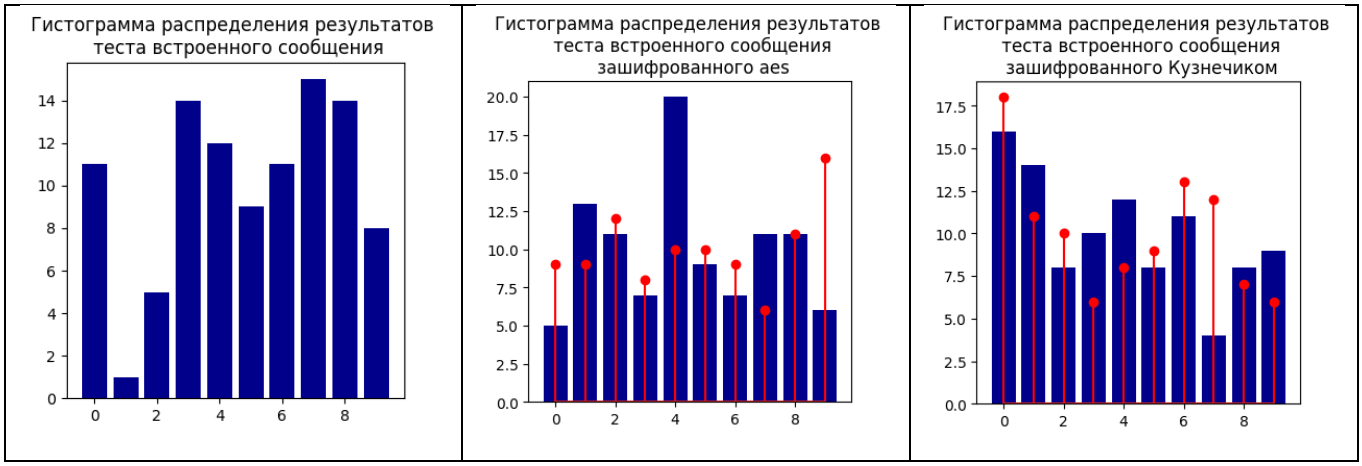


Рисунок П3.82 – Распределения значений результатов тестирования стегосистем

Фрагмент 3. Тест 1. Слой 1.

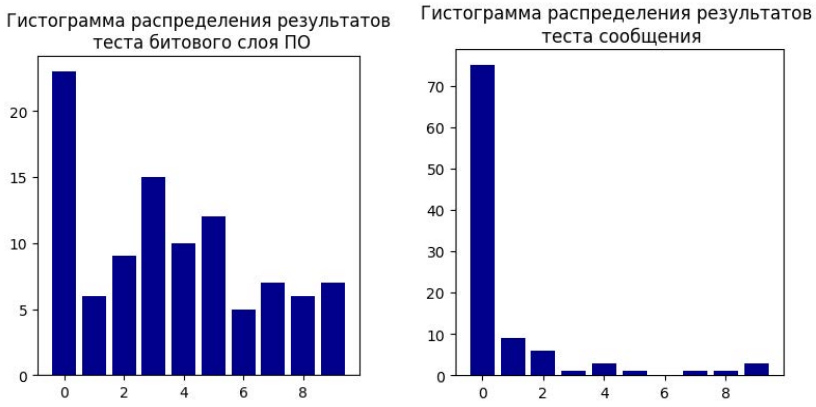


Рисунок П3.83 – Распределения значений результатов тестирования битового слоя и сообщения

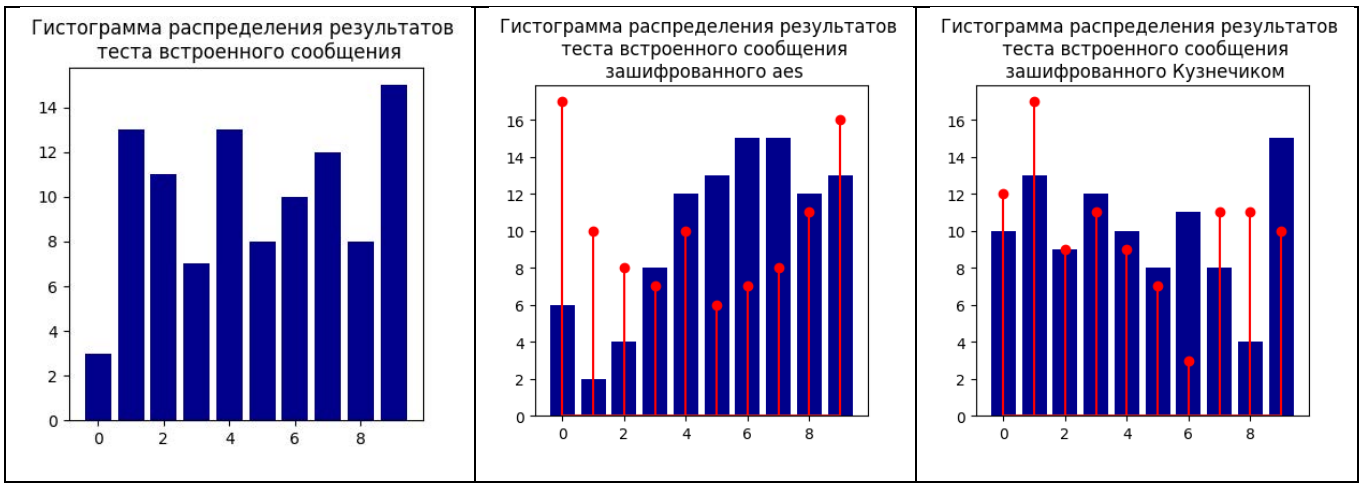


Рисунок П3.84 – Распределения значений результатов тестирования стегосистем

Фрагмент 3. Тест 1. Слой 2.

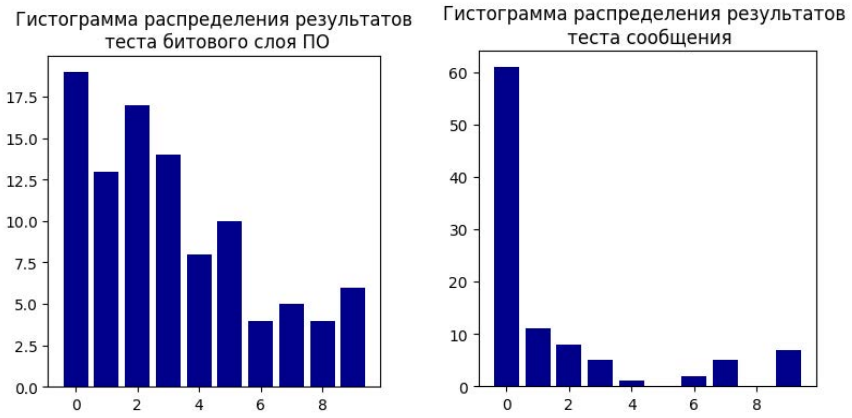


Рисунок П3.85 – Распределения значений результатов тестирования битового слоя и сообщения

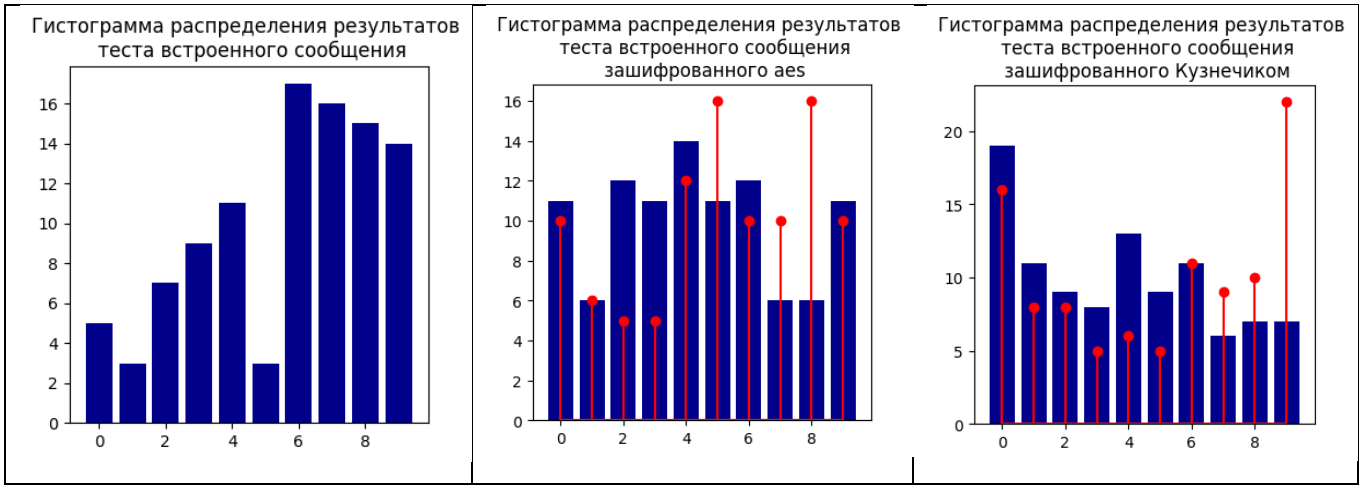


Рисунок П3.86 – Распределения значений результатов тестирования стегосистем

Фрагмент 3. Тест 1. Слой 3.

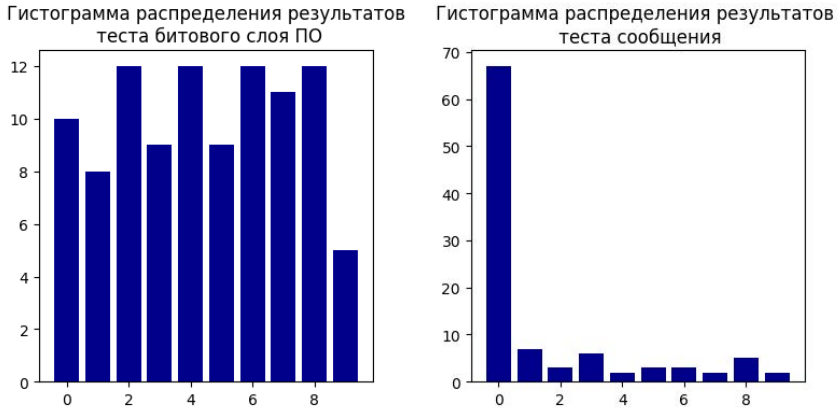


Рисунок П3.87 – Распределения значений результатов тестирования битового слоя и сообщения

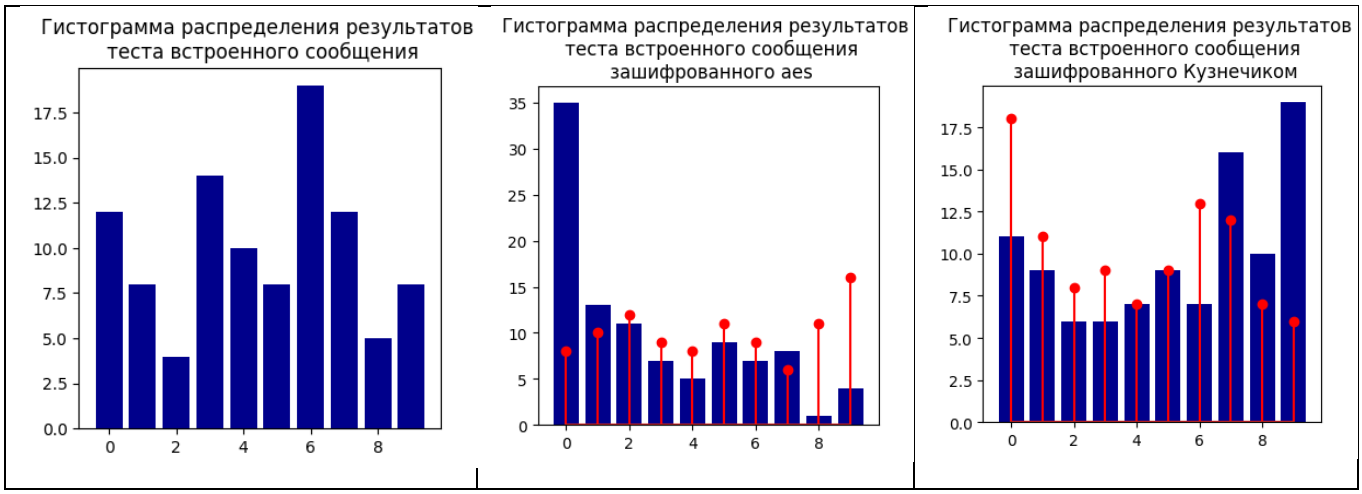


Рисунок П3.88 – Распределения значений результатов тестирования стегосистем

Фрагмент 4. Тест 1. Слой 0.

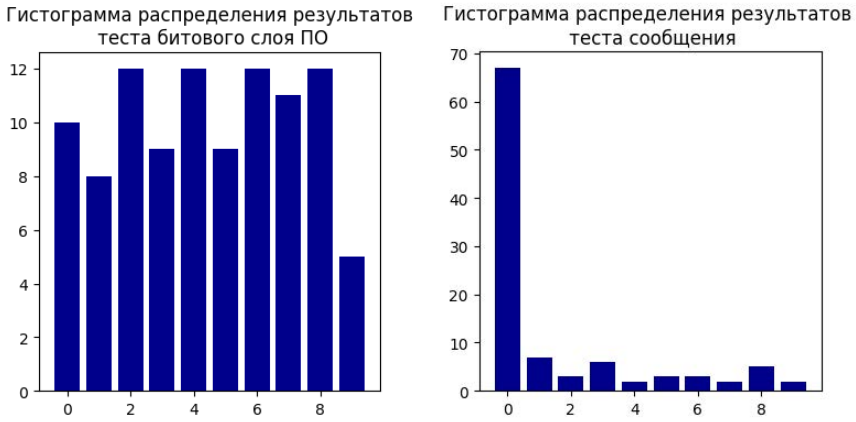


Рисунок П3.89 – Распределения значений результатов тестирования битового слоя и сообщения

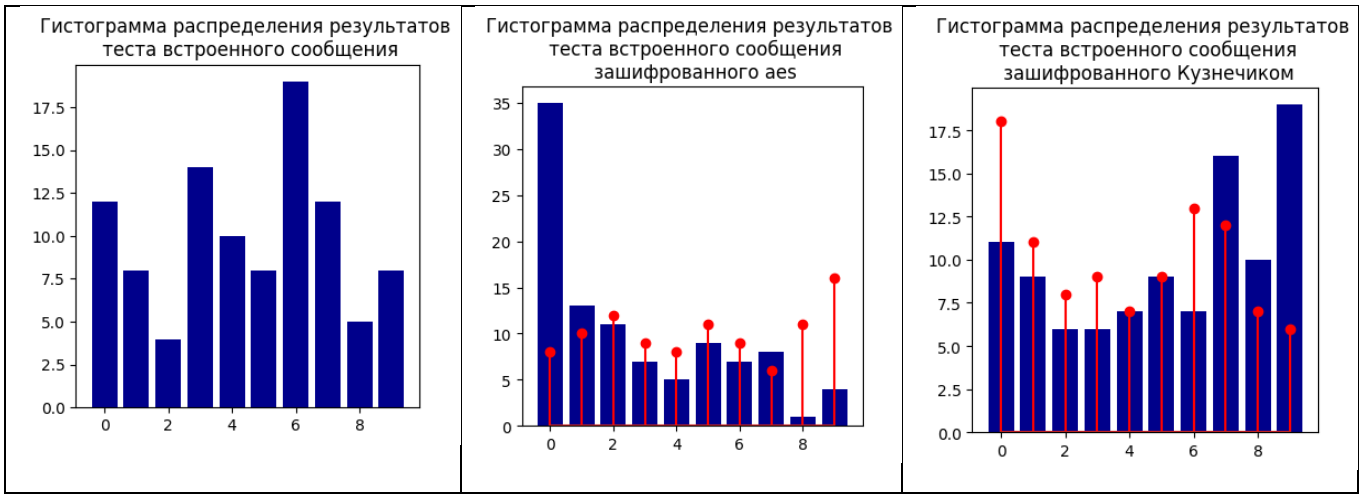


Рисунок П3.90 – Распределения значений результатов тестирования стегосистем

Фрагмент 4. Тест 12. Слой 1.

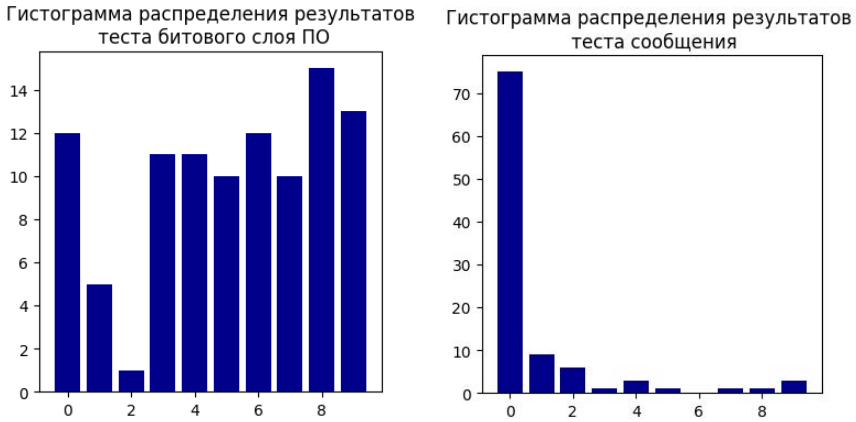


Рисунок П3.91 – Распределения значений результатов тестирования битового слоя и сообщения

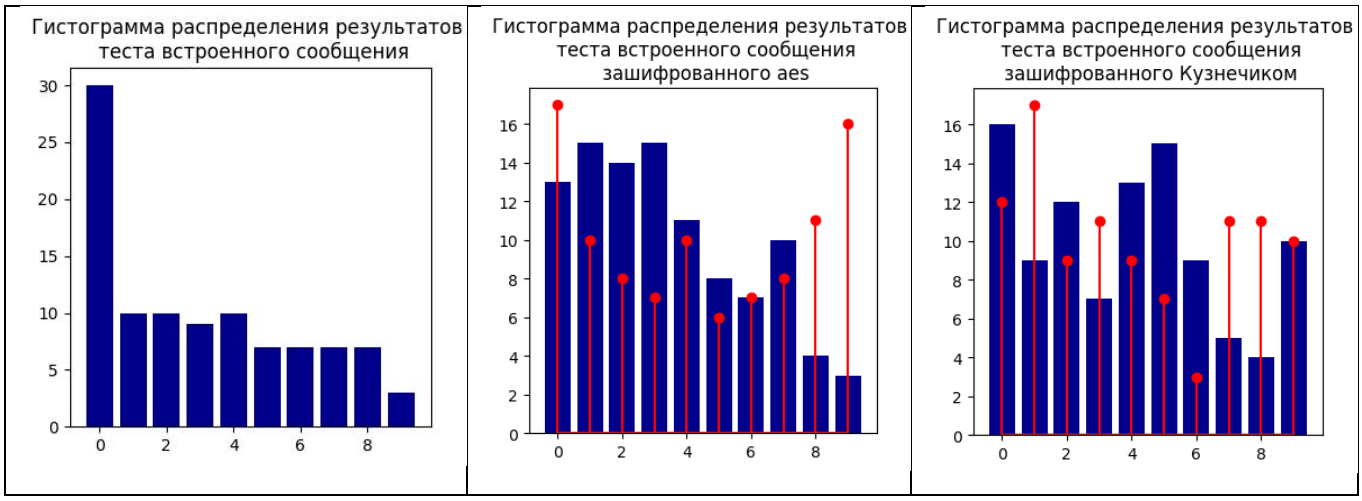


Рисунок П3.92 – Распределения значений результатов тестирования стегосистем

Фрагмент 4. Тест 1. Слой 2.

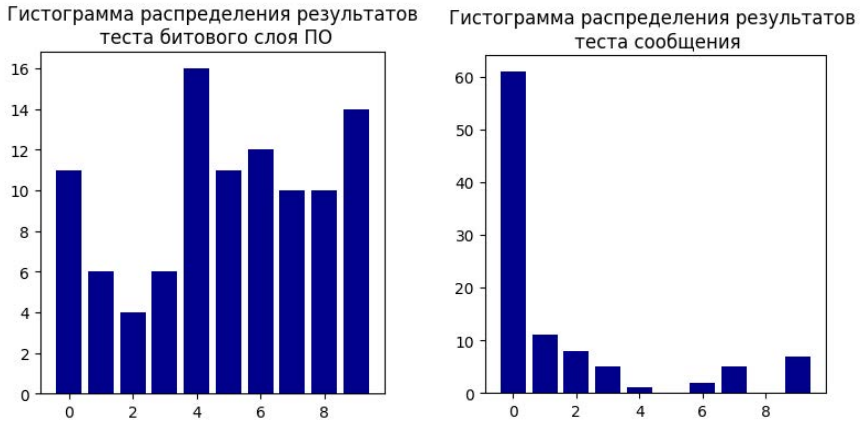


Рисунок П3.93 – Распределения значений результатов тестирования битового слоя и сообщения

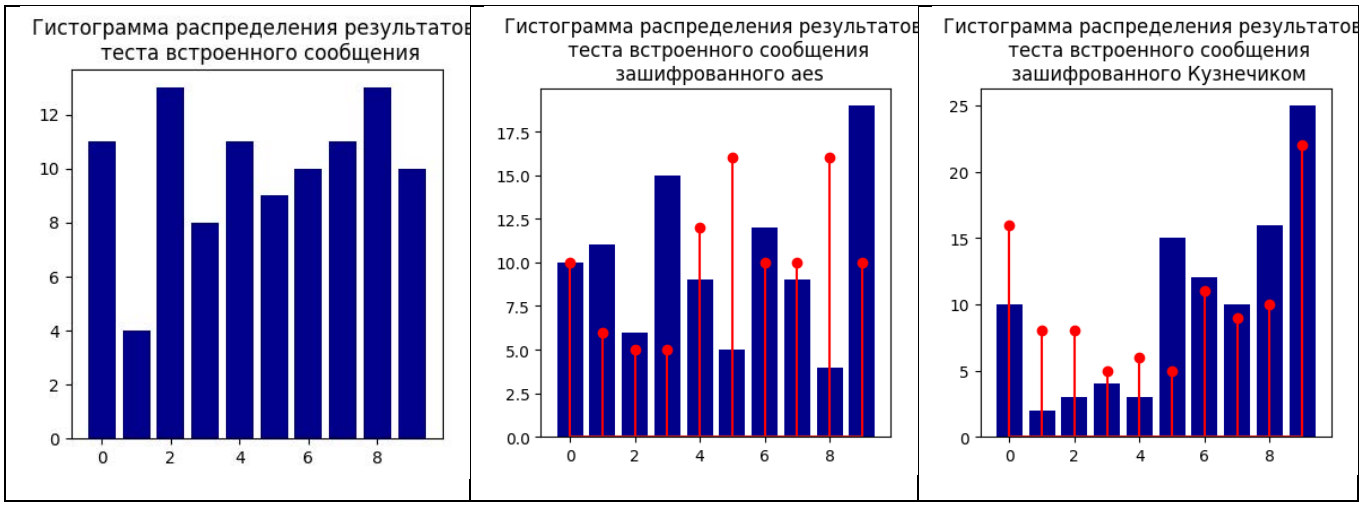


Рисунок П3.94 – Распределения значений результатов тестирования стегосистем

Фрагмент 4. Тест 12. Слой 3.

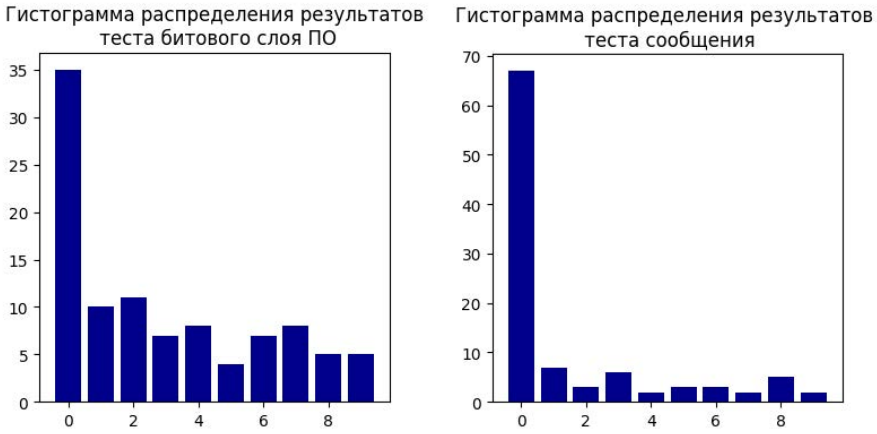


Рисунок П3.95 – Распределения значений результатов тестирования битового слоя и сообщения

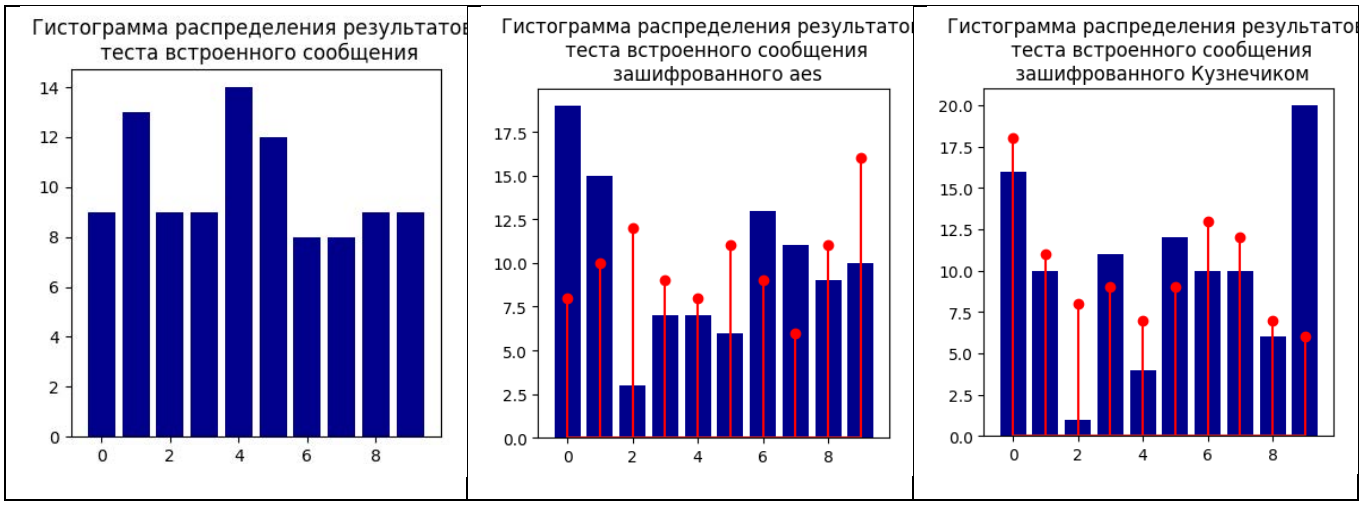


Рисунок П3.96 – Распределения значений результатов тестирования стегосистем