

4. Мендес В., Хэй Э. Мода с 1900 / В. Мендес, Э. Хэй. – М.: Ad Marginem, 2025. – 336 с.
5. Тер-Газарян О. Есенин и Айседора Дункан: одна душа на двоих / О. Тер-Газарян. – М.: Рипол-Классик, 2014. – 160 с.
6. Gastronomic Voyeurism: The South Korean trend that means you'll never eat alone. – URL: <https://www.independent.co.uk/tech/gastronomic-voyeurism-the-south-korean-trend-that-means-you-ll-never-eat-alone-9090847.html> (дата обращения: 02.10.2025).

УДК 004.056.5:004.032.6

## **СТЕГАНОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ АВТОРСКИХ ПРАВ НА ВИДЕОКОНТЕНТ В ЦИФРОВЫХ МЕДИА**

*Попеня Н. В.*

ст. преподаватель, магистр

Белорусский государственный технологический университет, г. Минск

Рассматривается проблема защиты авторских прав на мультимедийный контент в условиях современной цифровой среды. На основе анализа недостатков классических криптографических методов обоснована необходимость применения компьютерной стеганографии. Предложен комплексный метод многоуровневого встраивания цифровых водяных знаков в аудио- и видеопотоки, характеризующийся устойчивостью к сжатию и конвертации.

Ключевые слова: стеганография, защита авторских прав, видеоконтент, цифровые водяные знаки.

Защита авторских прав на мультимедийный контент является одной из ключевых проблем обеспечения информационной безопасности. Согласно статистическим данным, доля видеоконтента в мировом трафике продолжает неуклонно расти [1]. Высокая популярность формата и доступность средств его обработки приводят к увеличению числа случаев незаконного использования и модификации авторских материалов.

Существующие методы защиты, основанные на криптографии и разграничении доступа, обеспечивают безопасность данных лишь на этапах хранения и передачи. После декодирования контент становится уязвимым для незаконного распространения и модификации [2]. В связи с этим возникает необходимость применения стеганографических методов. В отличие от криптографии, скрывающей сам факт существования сообщения, стеганография позволяет незаметно

встраивать идентификационную информацию (цифровые водяные знаки) непосредственно в структуру медиаконтейнера [3]. Такие внедренные данные становятся неотъемлемой частью видеофайла, сохраняясь при его конвертации, сжатии и распространении.

Специфика видеостеганографии заключается в необходимости обработки огромных массивов данных в реальном времени и устойчивости к алгоритмам сжатия с потерями (MPEG, H.264/AVC и др.), которые удаляют избыточную информацию, обычно используемую для скрытия данных [4]. Видеопоток не является последовательностью независимых статических изображений, а представляет собой упорядоченную структуру кадров (GOP – Group of Pictures), связанных временными зависимостями [5].

Современные стандарты кодирования используют механизмы устранения межкадровой (временной) и внутрикадровой (пространственной) избыточности. Это создает существенные ограничения для встраивания скрытой информации. Большинство существующих методов, работающих в пространственной области (например, модификация LSB) и осуществляющих манипуляции непосредственно со значениями пикселей, не выдерживают перекодирования. Методы, работающие в частотной области (DCT, DWT), более устойчивы, так как модифицируют спектральные коэффициенты изображения, но требуют значительных вычислительных ресурсов, что затрудняет их применение в реальном времени.

Для решения задачи устойчивой защиты авторских прав разработан комплексный стеганографический метод, реализующий стратегию многоуровневого встраивания. Метод базируется на принципе избыточности и предполагает параллельное встраивание данных в аудиопоток (используя свойства слуховой системы человека) и видеопоток (используя особенности зрительного восприятия). Такое дублирование значительно повышает вероятность успешного извлечения авторской метки даже в случае атаки на одну из компонент медиафайла (например, удаление звуковой дорожки или перекодирование видеоряда).

Процесс защиты включает три последовательных этапа. Первоначальная подготовка данных определяет эффективность всего метода. На этой стадии формируется «цифровой паспорт» контента, включающий уникальные идентификаторы правообладателя и временные метки. Обработка включает сериализацию данных, симметричное шифрование для обеспечения конфиденциальности и при-

менение помехоустойчивого кодирования (коды Хэмминга) для исправления одиночных ошибок, возникающих при передаче [6].

На следующем этапе осуществляется обработка аудиопотока. Для аудиоканала используется адаптированный метод эхо-кодирования, заключающийся в добавлении к исходному сигналу его ослабленной копии. Ключевой особенностью является анализ огибающей сигнала: встраивание производится преимущественно в тихие фрагменты и паузы, что минимизирует слышимые искажения. Извлечение информации осуществляется посредством кепстрального анализа с применением адаптивного порога детектирования [7].

Завершающим шагом является встраивание информации в видеопоток, алгоритм которого учитывает структуру GOP и динамику сцены. С помощью анализа движения (оптический поток или разница кадров) определяются статичные области. Приоритет отдается опорным I-кадрам, так как их модификация не вызывает распространения искажений на зависимые кадры. Встраивание в такие области позволяет избежать визуальных артефактов, характерных для динамичных сцен при сжатии.

Рассматривая технические аспекты защиты видеоконтента, нельзя игнорировать их влияние на становление информационной культуры общества. Доступность цифровых инструментов меняет отношение общества к интеллектуальной собственности. Из-за технической легкости копирования произошло размытие границ между лицензионными материалами и свободно распространяемым контентом. Пользователь зачастую не может идентифицировать правообладателя, что снижает порог ответственности и способствует бесконтрольному распространению защищенной информации. Использование скрытой маркировки обеспечивает принцип неотвратимости ответственности в цифровой среде. Риск идентификации при незаконном распространении материалов побуждает к соблюдению установленных правовых рамок. Технология здесь выступает не как ограничитель свободы информации, а как инструмент, обеспечивающий баланс интересов между автором и обществом. Таким образом, внедрение данного решения выступает технологическим гарантом соблюдения авторских прав.

Разработанная методика и комплексный подход к защите прав интеллектуальной собственности на видеоконтент решает фундаментальное противоречие видеостеганографии – достиже-

ние компромисса между незаметностью скрытого сообщения и его устойчивостью к искажениям. Внедрение подобных технических решений создает надежную технологическую базу для реализации механизмов защиты авторского права.

*Список использованных источников*

1. Cisco Annual Internet Report (2018–2023) White Paper / Cisco Systems. — San Jose : Cisco Systems, 2020. — URL: <https://www.cisco.com> (date of access: 12.10.2025).
2. Digital watermarking and steganography / I. J. Cox [et al.]. — 2nd ed. — Burlington : Morgan Kaufmann, 2008. — 624 p.
3. Fridrich, J. Steganography in digital media : principles, algorithms, and applications / J. Fridrich. — Cambridge : Cambridge University Press, 2009. — 466 p.
4. Mstafa, R. J. A robust video steganography method based on motion analysis / R. J. Mstafa, K. M. Elleithy // LISAT '15 : proceedings of the IEEE Long Island Systems, Applications and Technology Conference, Farmingdale, NY, USA, 1–2 May 2015 / IEEE. — Farmingdale, 2015. — P. 1–6.
5. Richardson, I. E. The H.264 advanced video compression standard / I. E. Richardson. — 2nd ed. — Chichester : Wiley, 2010. — 350 p.
6. Попеня, Н. В. Методика подготовки и структура авторских данных для защиты видеофайла методами стеганографии / Н. В. Попеня // Труды БГТУ. Сер. 4, Принт- и медиатеchnологии. — 2025. — № 2 (297). — С. 71–77.
7. Попеня, Н. В. Метод аудиостеганографии для AAC-сжатых аудиосигналов на основе эхо-кодирования и адаптивного кепстрального анализа / Н. В. Попеня, Д. В. Романенко // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. — 2025. — № 2 (296). — С. 110–119.

УДК 316.77

**МЕДИАКОММУНИКАЦИИ В СИСТЕМЕ  
СРЕДНЕГО СПЕЦИАЛЬНОГО ОБРАЗОВАНИЯ:  
ИННОВАЦИОННЫЕ ПОДХОДЫ К ФОРМИРОВАНИЮ  
ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ**

*Ракитина А. В.*

Бобруйский механико-технологический колледж, г. Бобруйск

В научной работе рассматривается возрастающая значимость медиакоммуникаций как ключевого элемента образовательной среды в учреждениях уровня среднего специального образования. Оценена эффективность работы существующей информационной системы учреждения и определены перспективы её развития.

Ключевые слова: коммуникации, медиа, образование, информационная система.