УДК 004.056.55:004.6

Н. В. Попеня
Белорусский государственный технологический университет

МЕТОДИКА ПОДГОТОВКИ И СТРУКТУРА АВТОРСКИХ ДАННЫХ ДЛЯ ЗАЩИТЫ ВИДЕОФАЙЛА МЕТОДАМИ СТЕГАНОГРАФИИ

В статье рассматривается актуальная проблема защиты авторских прав на видеоинформацию с использованием методов компьютерной стеганографии. Подчеркивается критическая важность этапа подготовки встраиваемого сообщения, определяющего эффективность и надежность всего стегометода. Целью работы является разработка и описание методики формирования и предварительной обработки авторской информации для последующего скрытного и устойчивого встраивания в видеофайл. Детально анализируется состав авторской информации, необходимой для подтверждения прав (идентификаторы автора и контента, временные метки и др.). Предлагается формат структуризации данных, ориентированный на компактность. Описывается последовательность шагов подготовки: сериализация данных, применение помехоустойчивого кодирования на основе кодов Хэмминга для обеспечения целостности и возможности исправления одиночных битовых ошибок, использование симметричного шифрования для конфиденциальности встраиваемых данных. Обосновывается выбор применяемых подходов с точки зрения их влияния на итоговые характеристики сообщения (размер, стойкость к искажениям, защищенность). Подготовленное таким образом сообщение предназначено для дальнейшего встраивания в видеофайл с использованием разработанного автором комплексного стеганографического метода, сочетающего внедрение в аудио- и видеопотоки.

Ключевые слова: стеганография, защита авторских прав, видеоинформация, подготовка сообщения, авторская информация, коды Хэмминга, шифрование.

Для цитирования: Попеня Н. В. Методика подготовки и структура авторских данных для защиты видеофайла методами стеганографии // Труды БГТУ. Сер. 4, Принт- и медиатехнологии. 2025. № 2 (297). С. 71–77.
DOI: 10.52065/2520-6729-2025-297-10.

N. V. Popenya
Belarusian State Technological University

FORMATION AND PREPARATION OF COPYRIGHT INFORMATION DATA FOR STEGANOGRAPHIC PROTECTION OF VIDEO CONTENT

The article addresses the relevant issue of copyright protection for video information using computer steganography methods. The critical importance of the embedded message preparation stage, which determines the effectiveness and reliability of the entire steganographic method, is emphasized. The objective of the work is the development and description of a methodology for forming and preprocessing copyright information for subsequent covert and robust embedding into a video file. The composition of the copyright information necessary for rights verification (author and content identifiers, timestamps, etc.) is analyzed in detail. A data structuring format focused on compactness is proposed. The sequence of preparation steps is described: data serialization, application of error-correction coding based on Hamming codes to ensure integrity and the ability to correct single-bit errors, and the use of symmetric encryption for the confidentiality of the embedded data. The choice of the applied approaches is justified from the perspective of their impact on the final message characteristics (size, resistance to distortion, security). The message prepared in this way is intended for further embedding into a video file using the author's developed comprehensive steganographic method, which combines embedding into audio and video streams.

Keywords: steganography, copyright protection, video information, message preparation, copyright information, Hamming codes, encryption.

For citation: Popenya N. V. Formation and preparation of copyright information data for steganographic protection of video content. *Proceedings of BSTU, issue 4, Print- and Mediatechnologies*, 2025, no. 2 (297), pp. 71–77 (In Russian).
DOI: 10.52065/2520-6729-2025-297-10.

Введение. В современном мире цифровые технологии сделали создание, распространение и копирование видеоконтента чрезвычайно простым и доступным. Широкое распространение видеоматериалов в сети Интернет, социальных сетях, на стриминговых платформах и в системах обмена файлами одновременно обострило проблему защиты авторских прав [1]. Незаконное копирование, распространение и использование видеопродукции приводит к значительным финансовым потерям правообладателей и снижает интерес в созданию новых материалов.

Традиционные методы защиты, такие как системы управления цифровыми правами (DRM) и видимые цифровые водяные знаки (ЦВЗ), имеют свои ограничения. Системы DRM могут быть сложными для пользователей и зачастую поддаются обходу [2, с. 250–255], а видимые ЦВЗ снижают визуальное качество контента и могут быть удалены или искажены злоумышленниками [3, с. 88–92]. В этом контексте актуальным направлением становится использование методов компьютерной стеганографии.

Компьютерная стеганография занимается вопросами сокрытия самого факта передачи информации путем встраивания секретных данных (сообщений) в другие, несекретные данные (контейнеры), такие как изображения, аудио- или видеофайлы [4, с. 12; 5, с. 19–23]. В отличие от криптографии, которая защищает содержание сообщения, но не скрывает факта его наличия, стеганография стремится сделать скрытое сообщение незаметным для стороннего наблюдателя. Применительно к защите авторских прав стеганография позволяет встроить идентификационную информацию правообладателя непосредственно в медиафайл таким образом, чтобы она была невидима при обычном просмотре или прослушивании, но могла быть извлечена при необходимости подтверждения авторства [3, с. 155–160].

Однако эффективность и надежность любого стеганографического метода в значительной степени зависят не только от алгоритма встраивания и извлечения, но и от того, какая информация и в каком виде встраивается. Этап подготовки встраиваемого сообщения является критически важным. Неправильно подготовленное сообщение может:

– иметь слишком большой объем, что снижает возможную скрытность и устойчивость встраивания или делает его невозможным при ограниченной стеганографической емкости контейнера;

– быть уязвимым к обнаружению статистическими методами стегоанализа [5, с. 315–320];

– быть легко повреждено при незначительных искажениях контейнера (например, при сжатии видео), что сделает невозможным его корректное извлечение и интерпретацию;

– не содержать достаточной информации для однозначного подтверждения авторских прав [1].

Поэтому разработка методики формирования и предварительной обработки авторской информации, обеспечивающей ее компактность, конфиденциальность, целостность и информативность, является неотъемлемой частью создания надежной стеганографической системы защиты авторских прав. Применение помехоустойчивых кодов, таких как коды Хэмминга, позволяет повысить надежность извлечения данных в условиях возможных ошибок [6, с. 50–55], а использование современных алгоритмов шифрования, например AES, обеспечивает требуемый уровень конфиденциальности [7, с. 177–185].

Целью данной статьи является разработка и описание методики подготовки сообщения, содержащего авторскую информацию, для последующего скрытного и устойчивого встраивания в видеофайлы в рамках комплексного стеганографического метода защиты авторских прав.

Основная часть. Эффективность стеганографического метода защиты авторских прав напрямую зависит от качества и структуры встраиваемого сообщения. На данном этапе необходимо определить, какая именно информация должна быть включена в сообщение для надежного подтверждения авторства, и в каком формате ее следует представить для обеспечения компактности, однозначности и пригодности к последующей обработке (помехоустойчивому кодированию и шифрованию).

При формировании состава авторской информации для стеганографического встраивания необходимо найти баланс между информативностью и компактностью. С одной стороны, сообщение должно содержать достаточный объем данных для однозначной идентификации правообладателя и объекта авторского права. С другой стороны, его размер должен быть минимально возможным, чтобы не снижать скрытность встраивания и не превышать стеганографическую емкость контейнера, которая для видеофайлов, особенно после сжатия, может быть ограничена [3, с. 210–215].

Анализ законодательства об авторском праве, в частности Закона Республики Беларусь «Об авторском праве и смежных правах» [1], а также общепринятой практики идентификации контента позволяет выделить следующий минимально необходимый набор данных для включения в стеганографическое сообщение.

1. Идентификатор правообладателя (Author ID) – уникальный код или имя, позволяющие однозначно определить автора или текущего владельца прав на произведение. Это может быть как стандартизированный идентификатор (например, ISNI – International Standard Name Identifier,

если применимо и доступно [8]), так и внутренний идентификатор организации или псевдоним автора. Использование уникального идентификатора предпочтительнее простого имени для избежания неоднозначности.

2. Идентификатор произведения (Content ID) – уникальный код, присвоенный конкретному видеофайлу. Это может быть международный стандартный аудиовизуальный номер (ISAN [9]), если произведение зарегистрировано, или внутренний уникальный идентификатор, генерируемый системой защиты или правообладателем. Как вариант, для идентификации конкретной версии файла может использоваться криптографический хэш (например, SHA-256) исходного, немодифицированного видеофайла [7, с. 450–455]. Встраивание хэша позволяет не только идентифицировать контент, но и служить индикатором его целостности (любое изменение контента изменит и его хэш).

3. Временная метка (Timestamp) – дата и, возможно, время создания произведения или дата встраивания авторской информации. Этот параметр важен для установления приоритета прав и фиксации момента добавления защитной метки [1]. Рекомендуется использовать стандартный формат, например UNIX timestamp, для компактности и универсальности.

4. Символ охраны авторского права – общепринятый знак охраны авторского права «©» (Copyright symbol). Хотя его наличие не является обязательным условием возникновения авторского права согласно Бернской конвенции и законодательству Республики Беларусь [1], его включение служит общепринятым уведомлением о защите прав.

5. Год первой публикации/обнародования, когда произведение было впервые сделано доступным для публики. Это важный элемент для определения срока действия авторских прав [1].

6. Краткая информация о лицензии/условиях использования (License Info) – короткий код или флаг, указывающий на тип лицензии (например, «Все права защищены», код лицензии Creative Commons [10], «Только для некоммерческого использования»). Это поле следует использовать с осторожностью, чтобы не увеличивать размер сообщения.

7. Контрольная сумма сообщения (Message Checksum) – контрольная сумма (например, CRC32) самого формируемого сообщения перед шифрованием. Это позволит на этапе извлечения проверить целостность расшифрованных данных независимо от работы кодов коррекции ошибок, примененных к зашифрованному потоку.

Для надежной идентификации сторон правоотношения в сообщение необходимо включить уникальный идентификатор правообладателя (Author ID) и уникальный идентификатор самого произведения (Content ID). В качестве идентификаторов могут использоваться как стандартизованные коды, такие как ISNI [8] или ISAN [9], если они присвоены, так и внутренние коды организации или даже псевдонимы, при условии их уникальности. Для установления приоритета прав следует использовать временную метку (Timestamp) – дату создания или встраивания информации, а также общепринятые элементы уведомления об охране прав: символ охраны авторского права «©» и год первой публикации. В некоторых случаях целесообразно добавить краткую информацию о лицензии (License Info), например в виде кода, указывающего на тип лицензии Creative Commons [10], а также контрольную сумму сообщения (Message Checksum) для проверки целостности извлеченных данных. Однако при принятии решения о включении этих полей необходимо учитывать их влияние на общий размер сообщения.

Для представления этих данных необходимо выбрать формат, обеспечивающий максимальную компактность и простоту последующего парсинга (разбора) после извлечения и расшифровки. Текстовые форматы, такие как JSON или XML, обеспечивают хорошую читаемость и гибкость структуры, однако характеризуются высокой избыточностью, что неприемлемо для стеганографии. Формат «ключ-значение» является более компактным, но все еще требует хранения ключей. Поэтому для обеспечения максимальной компактности предпочтение отдается бинарному формату. Чтобы обеспечить некоторую гибкость и эффективность хранения идентификаторов и других данных переменной длины, целесообразно использовать бинарную структуру, в которой для каждого поля переменной длины указывается его тип и размер, или использовать комбинацию полей фиксированной и переменной длины. Примерная структура такого бинарного сообщения (с условными длинами полей) может выглядеть как последовательность байтов: тип AuthorID (1 байт), длина AuthorID (1 байт), значение AuthorID (*N* байт), тип ContentID (1 байт), длина ContentID (1 байт), значение ContentID (*M* байт), Timestamp (4 байта – UNIX time), флаги (1 байт – наличие ©, тип лицензии), год публикации (2 байта), CRC32 сообщения (4 байта).

В данной структуре *N* и *M* обозначают переменные длины (в байтах) полей «Значение AuthorID» и «Значение ContentID» соответственно, которые определяются значениями в предшествующих им полях «Длина AuthorID» и «Длина ContentID». Такая структура, при условии ее строгой спецификации для кодирования и декодирования, обеспечивает необходимый баланс информативности и компактности, создавая основу для последующих этапов кодирования и шифрования.

Сформированное бинарное сообщение, содержащее структурированную авторскую информацию, еще не готово к непосредственному встраиванию. Оно должно пройти этапы предварительной обработки для обеспечения его устойчивости к возможным ошибкам и для защиты его конфиденциальности.

Процесс стеганографического встраивания, а также последующая обработка медиаконтейнера (например, сжатие с потерями, перекодирование, передача по сетям с шумами) могут привести к возникновению ошибок в отдельных битах встроенного сообщения [5, с. 150–155]. Даже незначительное количество таких ошибок может сделать извлеченное сообщение нечитаемым или невалидным, что сведет на нет усилия по защите авторских прав. Для повышения надежности извлечения встраиваемого сообщения в условиях возможных ошибок, возникающих при стеганографическом встраивании или последующей обработке медиафайлов, необходимо применение методов помехоустойчивого кодирования. В рамках разрабатываемого метода для этой цели предлагается использовать коды Хэмминга. Выбор именно кодов Хэмминга обусловлен их относительной простотой реализации и хорошей эффективностью при исправлении одиночных битовых ошибок, которые являются наиболее вероятным типом искажений в данном контексте [6, с. 50–52; 11, с. 80–85]. Коды Хэмминга добавляют к информационным битам контрольные биты, вычисляемые по определенному алгоритму, что позволяет при декодировании не только выявить, но и исправить одиночную ошибку [12; 13, с. 60–75].

Применение кодов Хэмминга предполагает обработку всего сериализованного бинарного сообщения. Оно разбивается на блоки (например, по $k = 4$, 11 или 26 информационных бит), и к каждому блоку добавляются контрольные биты, формируя кодовое слово длиной n бит (соответственно, $n = 7$, 15 или 31). Этот процесс неизбежно приводит к увеличению общего размера сообщения, представляя собой компромисс между надежностью и объемом передаваемых данных. Величина этой избыточности (r/k, где r – число контрольных бит) напрямую зависит от выбора параметров кода.

Для количественной оценки влияния этапов кодирования и последующего шифрования на размер сообщения рассмотрим пример. Пусть исходное структурированное бинарное сообщение, содержащее идентификаторы автора и контента (по 8 байт каждый), временную метку (4 байта), флаги (1 байт), год публикации (2 байта) и контрольную сумму CRC32 (4 байта), имеет общий размер 31 байт (248 бит).

Применим к этому сообщению помехоустойчивое кодирование Hamming (15, 11). Исходные 248 бит информации потребуют 248 / 11 = 23 блока. Каждый блок из 11 информационных бит будет дополнен 4 контрольными битами до 15 бит. Общий размер после кодирования составит $23 \cdot 15 = 345$ бит, или 345 / 8 = 44 байта. Увеличение размера за счет ECC составит $(44 - 31) / 31 \approx 41{,}9\%$.

На следующем этапе к закодированному сообщению применяется шифрование AES-128 в режиме CBC, что требует добавления вектора инициализации (IV) размером 16 байт. Конечный размер сообщения, готового к встраиванию, составит 44 байта + 16 байт (IV) = 60 байт. Общее увеличение размера относительно исходного составляет $(60 - 31) / 31 \approx 93{,}5\%$.

В таблице представлены результаты расчетов для данного примера, а также для кодов Hamming (7, 4) и Hamming (31, 26), демонстрирующие зависимость итогового размера от выбора параметров помехоустойчивого кодирования.

Изменение размера сообщения на этапах подготовки

Параметры ECC	Исходный размер, байт	Размер после ECC, байт	Увеличение ECC, %	Размер после AES, байт	Общее увеличение, %
Hamming (7, 4)	31	55	77,4	71	129,0
Hamming (15, 11)	31	44	41,9	60	93,5
Hamming (31, 26)	31	39	25,8	55	77,4

Как следует из представленных расчетов, применение помехоустойчивого кодирования вносит основной вклад в увеличение размера подготовленного сообщения, при этом степень увеличения существенно зависит от выбора параметров кода Хэмминга. Так, использование кода с меньшей корректирующей способностью, но и меньшей избыточностью (Hamming (31, 26)), увеличивает общий размер сообщения на 77,4%, тогда как применение более избыточного кода (Hamming (7, 4)) приводит к увеличению размера на 129,0%. Шифрование добавляет постоянную избыточность за счет вектора инициализации (16 байт в данном случае). Итоговое увеличение размера сообщения, которое в рассмотренных примерах составляет от 71 до 129% от исходного, является необходимой платой за обеспечение конфиденциальности и надежности извлечения авторской информации. Оценка этой избыточности критически важна для определения пригодности подготовленного сообщения к встраиванию в конкретный медиаконтейнер с учетом его стеганографической емкости и ожидаемого уровня искажений.

Встроенная авторская информация, даже если сам факт ее наличия скрыт, не должна быть

доступна для прочтения и анализа неавторизованным лицам. Злоумышленник, сумевший извлечь скрытое сообщение, не должен иметь возможности понять его содержание или модифицировать его для своих целей. Для обеспечения конфиденциальности авторской информации необходимо применить криптографическое шифрование.

Предлагается использовать современный симметричный блочный алгоритм шифрования, такой как AES (Advanced Encryption Standard) [14, с. 299–310]. AES является международным стандартом шифрования, обеспечивает высокий уровень криптостойкости при использовании ключей достаточной длины (например, 128, 192 или 256 бит) и характеризуется хорошей производительностью на различных платформах. Выбор симметричного алгоритма обусловлен тем, что для извлечения и проверки авторской информации, как правило, используется тот же субъект (или его доверенная система), который осуществлял встраивание, что упрощает управление секретным ключом.

Шифрование применяется ко всему сообщению, уже прошедшему этап помехоустойчивого кодирования, т. е. шифруется последовательность битов, включающая как исходную информацию, так и добавленные контрольные биты кода Хэмминга. Для обеспечения большей стойкости к атакам рекомендуется использовать один из стандартизированных режимов шифрования, например CBC (Cipher Block Chaining) или CTR (Counter Mode) [15, с. 15–25]. Эти режимы добавляют элемент случайности в процесс шифрования, что делает зашифрованный текст менее предсказуемым, даже если в исходном сообщении есть повторяющиеся блоки. Использование режима CBC потребует также генерации и передачи (или встраивания) вектора инициализации (IV).

Ключевым аспектом использования шифрования является безопасное управление секретным ключом. Ключ должен быть известен только авторизованным сторонам (правообладателю или системе верификации) и должен надежно храниться. Вопросы генерации, распределения и хранения ключей выходят за рамки данной статьи, но их решение является необходимым условием для обеспечения реальной конфиденциальности данных.

В результате выполнения этапов помехоустойчивого кодирования и шифрования формируется итоговый битовый поток, готовый к передаче модулю стеганографического встраивания в аудио- или видеопотоки медиафайла. Этот поток обладает свойствами конфиденциальности (защищен шифрованием) и устойчивости к одиночным битовым ошибкам (благодаря кодам Хэмминга).

Заключение. В данной статье рассмотрен критически важный этап разработки стеганографической системы защиты авторских прав на видеоинформацию – формирование и подготовка встраиваемого сообщения. Актуальность данной задачи обусловлена необходимостью обеспечения не только скрытности самого факта наличия идентификационных данных в медиафайле, но и их конфиденциальности, целостности и информативности для надежного подтверждения прав собственности.

Предложена методика подготовки сообщения, включающая несколько последовательных этапов. Во-первых, определен состав необходимой авторской информации, содержащей идентификаторы правообладателя и контента, временные метки и другие релевантные данные, соответствующие требованиям законодательства Республики Беларусь об авторском праве [1]. Во-вторых, обоснован выбор компактного бинарного формата для структуризации этих данных, минимизирующего их объем, что является ключевым требованием для стеганографии. В-третьих, описаны этапы предварительной обработки: применение помехоустойчивого кодирования на основе кодов Хэмминга [6; 12] для повышения устойчивости сообщения к одиночным битовым ошибкам, возникающим в процессе встраивания или обработки видеофайла, и последующее шифрование с использованием алгоритма AES [14; 7] для обеспечения конфиденциальности встраиваемых данных. Обоснована последовательность применения этих этапов (кодирование перед шифрованием) для повышения общей надежности системы.

Проведен анализ влияния этапов подготовки на конечный размер сообщения. Показано, что внесение избыточности за счет помехоустойчивого кодирования и добавление вектора инициализации при шифровании приводят к увеличению объема данных, что является необходимым компромиссом для обеспечения надежности и безопасности. Предварительная оценка этого увеличения позволяет корректно выбирать параметры на этапе стеганографического встраивания.

Таким образом, предложенная методика подготовки авторской информации позволяет сформировать компактное, конфиденциальное и устойчивое к ошибкам сообщение, пригодное для последующего скрытного встраивания в видеоконтент. Детальная проработка этого этапа является неотъемлемой частью создания эффективной и надежной системы стеганографической защиты авторских прав.

Дальнейшие исследования в данном направлении могут включать оптимизацию структуры данных для еще большей компактности, исследование применения других, возможно, более эффективных помехоустойчивых кодов (например,

кодов Рида – Соломона для исправления пакетных ошибок), а также адаптацию параметров подготовки сообщения (выбор кода, длины ключа шифрования) в зависимости от характеристик медиаконтейнера и предполагаемого канала передачи или типа атак.

Список литературы

1. Об авторском праве и смежных правах: Закон Респ. Беларусь от 17 мая 2011 г. № 262-З : в ред. Закона Респ. Беларусь от 09.01.2023 г. № 243-З // Национальный правовой Интернет-портал Республики Беларусь. URL: https://pravo.by/document/?guid=3961&p0=H11100262 (дата обращения: 11.04.2025).

2. Rosenblatt B., Trippe B., Mooney S. Digital rights management. New York: M&T Books, 2002. 368 p.

3. Digital watermarking and steganography / I. J. Cox [et al.]. 2nd ed. Burlington: Morgan Kaufmann Publ., 2008. 598 p.

4. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. М.: Солон-Пресс, 2002. 272 с.

5. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. Киев: МК-Пресс, 2006. 288 с.

6. Блейхут Р. Теория и практика кодов, контролирующих ошибки / пер. с англ. К. Ш. Зигангирова. М.: Мир, 1986. 576 с.

7. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке С: пер. с англ. 2-е изд. М.: Триумф, 2002. 816 с.

8. Information and documentation – International standard name identifier (ISNI): ISO 27729:2012. Geneva: International Organization for Standardization, 2012. 28 p.

9. Information and documentation – International Standard Audiovisual Number (ISAN): ISO 15706-1:2002. Part 1: Audiovisual work identifier. Geneva: International Organization for Standardization, 2002. 22 p.

10. About The Licenses // Creative Commons. URL: https://creativecommons.org/licenses/ (date of access: 11.04.2025).

11. Lin S., Costello D. J. Jr. Error control coding: fundamentals and applications. 2nd ed. Englewood Cliffs: Prentice-Hall, 2004. 648 p.

12. Hamming R. W. Error detecting and error correcting codes // Bell System Technical Journal. 1950. Vol. 29, no. 2. P. 147–160.

13. Peterson W. W., Weldon E. J. Jr. Error-correcting codes. 2nd ed. Cambridge: MIT Press, 1972. 572 p.

14. FIPS PUB 197. Advanced Encryption Standard (AES) / National Institute of Standards and Technology. Gaithersburg, MD, 2001. 52 p.

15. Dworkin M. Recommendation for Block Cipher Modes of Operation: Methods and Techniques (NIST Special Publ. 800-38A). Gaithersburg, MD: NIST, 2001. 68 p.

References

1. On Copyright and Related Rights: Law of the Rep. of Belarus, May 17, 2011, no. 262-Z : as amended Jan 09, 2023, no. 243-Z. Available at: https://pravo.by/document/?guid=3961&p0=H11100262 (accessed 11.04.2025) (In Russian).

2. Rosenblatt B., Trippe B., Mooney S. Digital rights management. New York, M&T Books, 2002. 368 p.

3. Cox I. J., Miller M. L., Bloom J. A., Fridrich J., Kalker T. Digital watermarking and steganography (2nd ed.). Burlington, Morgan Kaufmann Publ., 2008. 598 p.

4. Gribunin V. G., Okov I. N., Turintsev I. V. *Tsifrovaya steganografiya* [Digital Steganography]. Moscow, Solon-Press Publ., 2002. 272 p. (In Russian).

5. Konakhovich G. F., Puzyrenko A. Yu. *Komp'yuternaya steganografiya. Teoriya i praktika* [Computer Steganography. Theory and Practice]. Kyiv, MK-Press Publ., 2006. 288 p. (In Russian).

6. Blahut R. E. Theory and Practice of Error Control Codes. Reading, MA, Addison-Wesley, 1983. 576 p.

7. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd ed.). New York, John Wiley & Sons, 1996. 784 p.

8. ISO 27729:2012. Information and documentation – International standard name identifier (ISNI). Geneva, International Organization for Standardization. 2012. 28 p.

9. ISO 15706-1:2002. Information and documentation – International Standard Audiovisual Number (ISAN) – Part 1: Audiovisual work identifier. Geneva, International Organization for Standardization. 2002. 22 p.

10. About The Licenses. Creative Commons. Available at: https://creativecommons.org/licenses/ (accessed 11.04.2025).

11. Lin S., Costello D. J. Jr. Error control coding: fundamentals and applications (2nd ed.). Englewood Cliffs, Prentice-Hall Publ., 2004. 648 p.

12. Hamming R. W. Error detecting and error correcting codes. *The Bell System Technical Journal*, 1950, no. 29 (2), pp. 147–160.

13. Peterson W. W., Weldon E. J. Jr. Error-correcting codes (2nd ed.). Cambridge, MIT Press, 1972. 572 p.

14. National Institute of Standards and Technology (NIST). FIPS PUB 197. Advanced Encryption Standard (AES). Gaithersburg, MD, 2001. 52 p.

15. Dworkin M. Recommendation for Block Cipher Modes of Operation: Methods and Techniques (NIST Special Publication 800-38A). Gaithersburg, MD, National Institute of Standards and Technology, 2001. 68 p.

Информация об авторе

Попеня Наталья Владимировна – аспирант кафедры информатики и веб-дизайна. Белорусский государственный технологический университет (ул. Свердлова, 13а, 220006, г. Минск, Республика Беларусь). E-mail: popenya@belstu.by

Information about the author

Popenya Natalya Vladimirovna – PhD student, the Department of Information Systems and Technologies. Belarusian State Technological University (13a Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: popenya@belstu.by

Поступила 20.04.2025