График наглядно демонстрирует сокращение времени проверки более чем в 5 раз.

Разработанный метод автоматизированного тестирования знаний на основе семантического анализа текстовых ответов демонстрирует высокую практическую и научную значимость. Интеграция NLP-моделей позволяет перейти от формальной проверки к оценке смыслового содержания ответов, что существенно повышает качество контроля знаний.

Дальнейшие исследования целесообразно направить на повышение интерпретируемости решений NLP-моделей и внедрение локальных специализированных языковых моделей для снижения зависимости от внешних сервисов.

ЛИТЕРАТУРА

1. Ржеутская Н.В. Сравнительная характеристика моделей и методов оценки знаний студентов // Цифровая трансформация. 2023. №4 (25). С. 32–41.

2. Гурин Н. И., Ржеутская Н. В. Структура семантической базы знаний для системы тестирования на естественном языке // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. 2025 № 1 (278). С.56-61..

3. FastAPI [Электронный ресурс]. – Режим доступа: https://fastapi.tiangolo.com/ru/ (дата обращения: 07.01.2026).

4. OpenAI API Documentation [Электронный ресурс]. – Режим доступа: https://platform.openai.com/docs/api-reference (дата обращения: 07.01.2026).

УДК 004.021

Е.А. Блинова, канд. техн. наук, зав. кафедрой ИСиТ,
О.А. Нистюк, ст. преп. (БГТУ, г. Минск)

## МЕТОД СТЕГАНОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИИ В STEP-ФАЙЛАХ

Стеганография – область науки, занимающаяся методами сокрытия факта передачи информации, часто применяемая для обеспечения конфиденциальности, защиты авторских прав, а также маркировки цифровых данных [1]. Стеганографические контейнеры представлены множеством различных форматов: это векторные и растровые изображения, звуковые и видео файлы, электронные текстовые документы. Для многих документов актуальна задача защиты авторских прав и подтверждения целостности документа.

Объектом исследования являются файлы векторных изображений, содержащих в своем описании объекты в виде совокупности нескольких функций, каждая из которых задана на каком-то множестве значений аргумента, то есть сплайна. Такие файлы широко используются в веб-графике, графическом дизайне, для создания иллюстраций с плавными кривыми, а также инженерных и архитектурных планов.

Одним из наиболее распространенных форматов в мире инженерии и промышленного дизайна является STEP (Standard for the Exchange of Product model data) – международный стандарт для обмена данными между различными системами инженерного проектирования. Главное назначение формата STEP – сохранить полную информацию о модели без потерь. Формат не является проприетарным, и может свободно использоваться различными приложениями, сохраняет точную геометрию, а также метаданные (материалы, допуски, структуру сборки, историю изготовления). Несмотря на то, что формально файл STEP – это изображение, по сути, это текстовый файл, который описывает модель на специальном языке EXPRESS. Формат поддерживает широкий спектр сущностей для отображения кривых, таких как базисные сплайны (b_spline_curve_with_knots), сплайновые поверхности (b_spline_surface_with_knots) и более простые элементы, например, окружность, эллипс, составные кривые и ломаные линии.

Основными преимуществами формата STEP являются точность, возможность использования в различном ПО и функциональность, так как файл может содержать и атрибутивные данные. В качестве недостатков указываются большой размер файла, отсутствие параметрической истории и сложность.

При разработке метода основными критериями эффективности являются незаметность (визуальные и функциональные изменения в 3D-модели должны отсутствовать), надежность (внедренная информация должна храниться при стандартном редактировании файла, например, перемещения элементов или изменении материалов) и вместимость (возможность внедрить достаточный объем данных, например, имя автора, дату создания или короткий идентификационный код).

Каждый .step файл строится на следующих основных сущностях:

1. CARTESIAN_POINT – это основная сущность для задания точки в пространстве тремя координатами (X, Y, Z). Она является главным кандидатом для стеганографии, поскольку изменять наименее значимый бит в числе с плавающей запятой (или высокой точности) в координате визуально незаметно.

2. DIRECTION – задает вектор направления в пространстве. Менее популярна для вмешательства, но также содержит числа, которые определяют компоненты вектора.

3. VECTOR – определяет вектор через его направление (DIRECTION) и величину (LENGTH). Величина может быть числом.

4. VERTEX_POINT – точка вершины геометрической фигуры. Ссылается на CARTESIAN_POINT, не содержит непосредственно числовых значений.

Можно сделать вывод, что CARTESIAN_POINT является лучшим вариантом для внедрения информации в файл. Обычно такие точки содержат три координаты, что позволяет вместить три бита сообщения, а каждая из этих координат имеет точность до 16 знаков после запятой, а потому изменения не будут заметны визуально.

Один из ключевых этапов разработки – реализация механизма проверки емкости контейнера. Метод должен учитывать максимальный объем данных, который может быть спрятан в конкретном STEP-файле на основе количества пригодных для вмешательства числовых полей. Если размер сообщения (включая служебные данные для декодирования) превышает эту границу, пользователю необходимо выбрать другой файл-контейнер. Это гарантирует корректность работы метода и избегает ошибок во внедрении и извлечении информации.

Разработка будет состоять из следующих ключевых этапов. Сначала будет проведен анализ структуры STEP-файла (стандарт ISO 10303-21) для идентификации секций и полей, наиболее подходящими для вмешательства – это числовые параметры с высокой точностью (например, координаты точек), где изменение младшего бита будет минимальным. Затем будет разработано ядро метода, которое реализует адаптированный LSB-подход для текстового представления чисел, учитывая необходимость сохранения синтаксиса файла. Для повышения криптостойкости был интегрирован дополнительный этап предварительной обработки сообщения с использованием симметричного шифрования и псевдослучайного распределителя на основе криптографического ключа для выбора мест вставки, что делает обнаружение факта вмешательства статистически сложнее [2].

Алгоритм внедрения информации:

1. Выделение массива со всеми точками из файла-контейнера.

2. Удаление из массива n точек, которые содержат целые числа.

3. Перемешивание точек на основе seed (ключ).

4. Разбиение сообщения на блоки и внедрение блока в точку.

5. Для каждого бита блока в соответствующей ему координате меняется два наименее значимых бита – последний заменяется на 1, предпоследний на бит сообщения.

6. Новый массив точек записывается в файл.

Алгоритм извлечения информации:

1. Выделение массива со всеми точками из файла-контейнера.

2. Удаление из массива n точек, которые содержат целые числа.

3. Перемешивание точек на основе seed.

4. Формирование сообщения с предпоследнего бита каждой координаты.

5. Обрезать часть данных по длине, равной полученному значению.

Таким образом, на основании проведенного анализа можно сделать вывод, что для реализации стеганографического внедрения в STEP-файлы наиболее оптимальным подходом является комбинация адаптированного метода LSB для работы с цифровыми координатами CARTESIAN_POINT и дополнительных криптографических механизмов для повышения общей стойкости системы. Выбор именно данных координат основан их высокой точностью, широким распространением, а также минимальным визуальным влиянием на модель при манипуляции с младшими битами.

ЛИТЕРАТУРА

1. Урбанович П.П. Защита информации методами криптографии, стеганографии и обфускации: учебно-метод. пос. для студ. вузов / П. П. Урбанович. – Минск: БГТУ, 2016. – 219 с.

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

УДК 003.26

А.Н. Николайчук, ассист.;
(БГТУ, г. Минск)

## ОБНАРУЖЕНИЕ СТЕГАНОГРАФИЧЕСКИХ УГРОЗ НА ОСНОВЕ АНАЛИЗА АНОМАЛИЙ В СЕТЕВОМ ТРАФИКЕ С ИСПОЛЬЗОВАНИЕМ IDS/IPS

В современной сфере информационной безопасности защита данных традиционно фокусируется на криптографии (шифровании) и противодействии вредоносному ПО. Однако существует класс угроз, связанных со скрытием самого факта передачи информации – сетевая стеганография [1]. Стеганографические методы не нарушают целост-