З технічного погляду параметри подання тексту є складовою мультимедійної системи, яка формує зручне та ергономічне візуальне середовище. Їх оптимізація розглядається не лише як питання дизайну, а як інструмент підвищення ефективності сприйняття інформації у цифровому просторі.

Продумане налаштування параметрів подання тексту є основою якісного процесу швидкочитання. Воно забезпечує не тільки зростання темпу, а й підтримання рівня розуміння, зорового комфорту та стабільної концентрації уваги. Таке поєднання фізіологічних і візуальних чинників створює умови для формування стійкої навички ефективного сприйняття тексту.

АЛГОРИТМИ СТИСНЕННЯ ТА ПЕРЕДАЧІ ВІДЕОКОНТЕНТУ НА ПЛАТФОРМІ YOUTUBE. СТЕГАНОГРАФІЯ ПРИ ПЕРЕДАЧІ ВІДЕО

І. О. Гриценко, Р. О. Бобнєв, ХНУРЕ, м. Харків

У сучасну цифрову епоху відеоконтент став одним з основних способів передачі інформації, розваг та навчання. Однією з найпопулярніших платформ для обміну відео є YouTube, який щодня обслуговує мільярди користувачів у всьому світі. Для забезпечення швидкої, якісної та економної передачі відео платформа використовує потужні алгоритми стиснення. Паралельно з цим, усе більш актуальною стає технологія прихованої передачі даних – стеганографія. У даній роботі розглянуто сучасні алгоритми стиснення відео, які застосовує YouTube, а також можливості використання стеганографії у відеофайлах.

Розглянемо процев стиснення. Коли користувач завантажує відео на YouTube, воно автоматично перекодовується — тобто проходить через алгоритми стиснення, що дозволяють зменшити розмір файлу без значно помітної втрати якості. Це необхідно для зниження навантаження на сервери та забезпечення швидкого потокового відтворення на різних пристроях [1].

H.264/AVC. Це один з найпоширеніших відеокодеків, який забезпечує добрий баланс між якістю відео та його розміром. Він використовує як внутрішньокадрове (intra-frame), так і міжкадрове (inter-frame) стиснення. Недолік полягає в тому, що має відносно менш ефективне стиснення у порівнянні з новішими кодеками, але перевага в тому що є найстаршим стандартом, а отже може працювати на більш старіших девайсах[2].

VP9. Розроблений компанією Google як безкоштовна альтернатива H.265. YouTube активно використовує VP9 для стиснення відео високої роздільної здатності (наприклад, 4K). Основна перевага — ефективніше стиснення без помітної втрати якості [3].

AV1. Найновіший відеокодек, що пропонує ще ефективніше стиснення у порівнянні з VP9. Підтримка AV1 поступово впроваджується на YouTube. Він дозволяє зменшити трафік при збереженні високої якості відео, однак вимагає більших обчислювальних ресурсів при кодуванні[4].

YouTube використовує технологію DASH (Dynamic Adaptive Streaming over HTTP), також відому як MPEG-DASH. Відео передається не суцільним потоком, а у вигляді невеликих сегментів, які змінюють свою якість у режимі реального часу залежно від швидкості з'єднання користувача. Це дозволяє мінімізувати буферизацію та забезпечити безперервне відтворення відео[5].

Стеганографія — це процес приховування інформації в цифрових медіафайлах (зображеннях, аудіо, відео), таким чином, щоб сторонній спостерігач не помітив самого факту передачі повідомлення. На відміну від криптографії, де основна мета — приховати зміст повідомлення, стеганографія намагається замаскувати його існування[6].

LSB (Least Significant Bit). Це найпростіший метод, який передбачає заміну найменш значущих бітів у кожному пікселі відео. Наприклад, заміна останнього біта у значеннях R, G, B кольорів пікселя. Людське око практично не вловлює таких змін.

Метод на основі DCT (дискретного косинус-перетворення). Застосовується для форматів, які використовують частотне стиснення (наприклад, MPEG). Дані вшиваються у високочастотні компоненти відео, які менш помітні для сприйняття.

Motion Vector Modulation. Метод зміни векторів руху, які використовуються під час стиснення відео (особливо в H.264). Вектори руху змінюються несуттєво, але цілеспрямовано — це дозволяє закодувати приховану інформацію.

Хоча стеганографія у відео можлива, її реалізація через YouTube неможлива. Це пов'язано з тим, що при завантаженні відео на платформу відбувається повторне кодування, яке змінює структуру відеофайлу. Тому стеганографію доцільно використовувати у локальних відеофайлах або при безпосередній передачі через файлів[7].

В інтернеті є доступ до програм що зроблять стеганографію, де можна у фотографії приховати інше фото, або так само з відео. На такому сайті як Github можна знайти багато різних програм які можуть провести стеганографію[8].

Як приклад використання, у 2020 році компанія з безпеки електронної комерції Sansec опублікувала звіт про виявлення шкідливого програмного забезпечення на різних сторінках оформлення замовлення. Таке шкідливе програмне забезпечення призначене для сканування кредитних карток та вилучення інших даних користувачів з веб-сайтів, і в цьому випадку воно було приховано у візуальних елементах у форматі SVG [9].

Стиснення відео — ключова технологія, яка дозволяє YouTube ефективно доставляти відеоконтент мільйонам користувачів по всьому світу. Використання сучасних кодеків (H.264, VP9, AV1) забезпечує високу якість відео навіть при низькій швидкості Інтернету.

Стеганографія у відео є цікавим напрямом цифрової безпеки, який дозволяє передавати приховану інформацію. Проте застосування стеганографії на YouTube обмежене через агресивне перекодування файлів. Для ефективного

використання стеганографії у відео рекомендується уникати платформ з повторною компресією, а натомість використовувати локальні файли або прямий обмін.

Список використаних джерел

1. Conaticus. The SECRET Algorithm Behind YouTube Compression. URL: https://youtu.be/xhroAm5XvU0?si=pu5aIO3mwaSn8qr8 (Дата звернення 04.04.2025 рік)
2. Cloudflare. What is H.264? | Advanced Video Coding (AVC). URL: https://www.cloudflare.com/learning/video/what-is-h264-avc/ (Дата звернення 07.04.2025 рік)
3. Andy Francis. VP9 Codec: The Complete Guide to Google's Open Source Video Codec. URL: https://bitmovin.com/blog/vp9-codec-status-quo/ (Дата звернення 07.04.2025 рік)
4. Alliance for Open Media. AV1 Video Codec. URL: https://aomedia.org/specifications/av1/ (Дата звернення 07.04.2025 рік)
5. Momento docs. What is DASH (Dynamic Adaptive Streaming over HTTP)?. URL: https://docs.momentohq.com/media-storage/performance/adaptive-bitrates/dash (Дата звернення 09.04.2025 рік)
6. Liu Y., Liu S. Neurocomputing // Video steganography: A review. - 2019. - 335. - p.238-250.
7. Kunhoth J., Subramanian N. Multimedia Tools and Applications // Video steganography: recent advances and challenges. - 2023. - 82. - p.41943–41985.
8. Anilsathyan. Deep-Video-Steganography-Hiding-Videos-in-Plain-Sight. URL: https://github.com/anilsathyan7/Deep-Video-Steganography-Hiding-Videos-in-Plain-Sight (дата звернення 23.04.2025)
9. NordVPN. Steganography explained: Meaning, types, and examples. URL: https://nordvpn.com/uk/blog/what-is-steganography/ (дата звернення 25.04.2025)

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ І ЗАПОБІГАННЯ КІБЕРАТАКАМ У РАДІОЗВ'ЯЗКУ

О. О. Дрождік, А. С. Єськова, к.т.н., проф. М. М. Колендовська, ХНУРЕ, м. Харків, Україна

В епоху цифрових технологій радіозв'язок є одним із найважливіших засобів передачі інформації, широко застосовуваним у телекомунікаціях, військових системах, Інтернеті речей (IoT) та інших сферах. Водночас, зростання кіберзагроз і складність атак на радіотехнології підвищують вимоги до безпеки інформації. В таких умовах штучний інтелект (ШІ) стає потужним інструментом для виявлення й запобігання кібератакам, що спрямовані на радіозв'язок. Метою даного дослідження є аналіз сучасних методів