НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Навчально-науковий інститут телекомунікаційних систем

Кафедра інформаційних технологій в телекомунікаціях

До захисту допущено:
В.О. завідувача кафедри
_____ Валерій ПРАВИЛО
«_____»_____2026 р.

ДИПЛОМНА РОБОТА
на здобуття ступеня бакалавра

за освітньо-професійною програмою «Інформаційно-комунікаційні технології»
спеціальності 172 Телекомунікації та радіотехніка

на тему: Модифікована система захисту контенту комерційних прямих трансляцій

Виконав : здобувач вищої освіти 4 курсу, групи ТІ-22
Миронюк Ілля Анатолійович _____

Науковий керівник: старший викладач кафедри
ІТТ НН ІТС Курдеча Василь Васильович _____

Рецензент: доцент кафедри ТК НН ІТС
кандидат технічних наук, доцент
Авдєєнко Гліб Леонідович _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Здобувач вищої освіти _____

Київ – 2026 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

Навчально-науковий інститут телекомунікаційних систем

Кафедра інформаційних технологій в телекомунікаціях

Рівень вищої освіти – перший (бакалаврський)
Освітньо-професійна програма «Інформаційно-комунікаційні технології» спеціальності 172 Телекомунікації та радіотехніка

ЗАТВЕДЖУЮ
В.О. завідувача кафедри
_____ Валерій ПРАВИЛО
«_____»_____2026 р.

ЗАВДАННЯ

на дипломну роботу студенту

Миронюку Іллі Анатолійовичу

1. Тема дипломної роботи: Модифікована система захисту контенту комерційних прямих трансляцій, старший викладач кафедри ІТТ НН ІТС Курдеча Василь Васильович - затверджені наказом по університету від 26.05.2026р. №1912-с.
2. Строк подання студентом дипломної роботи 06.06.2026 р.
3. Об’єкт дослідження: Процес захисту відеоданих від лнезаконної редистрибуції під час потокового передавання в реальному часі.
4. Вихідні дані до роботи: Існуючі захисти прямих трансляцій. Адтований до задач метод дихотомії.
5. Перелік завдань, які потрібно розробити:

Задачі дослідження:

1) Проаналізувати проблемні питання комерційних прямих трансляцій.

2) Проаналізувати наявні рішення захисту контенту.

3) Модифікувати систему захисту комерційних трансляцій із застосуванням ітеративного алгоритму маркування зображення на стороні сервера.

4) Оцінити ефективність запропонованого рішення.л

6. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо):

7. Дата видачі завдання: 24.09.2026

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Узгодження організаційних питань з науковим керівником	08.12.2025-12.12.2025	Виконано
2	Узгодження теми роботи та початок роботи над першим розділом	15.12.25-16.12.24	Виконано
3	Робота над першим, другим та третім розділами	05.01.2026-02.02.2026	Виконано
4	Робота над четвертим розділом. Планування розробки власного рішення	09.02.2026-17.02.2026	Виконано
5	Розробка власного рішення та його перевірка	23.02.2026-02.03.2026	Виконано
6	Підготовка п’ятого розділу	16.03.2026-30.03.2026	Виконано
7	Висновки про ефективність рішення	01.04.2026-14.04.2026	Виконано
8	Оформлення дипломної роботи	01.04.2026-14.04.2026	Виконано
9	Підготовка презентації до захисту	15.04.2026-31.04.2026	Виконано

Здобувач вищої освіти _____ Ілля МИРОНЮК

Науковий керівник роботи _____ Василь КУРДЕЧА

РЕФЕРАТ

Дипломна робота «Модифікована система захисту контенту комерційних прямих трансляцій» містить 54 сторінку тексту, 9 рисунків та 5 таблиць, а також використовує 25 літературних джерела посилання.
Актуальність теми: захист цифрового медіаконтенту комерційних прямих трансляцій є ключовим аспектом збереження економічної моделі OTT-провайдерів та правовласників, що визначає стійкість усієї галузі стрімінгу. В умовах стрімкого зростання обсягів незаконної редистрибуції контенту глобальні фінансові втрати правовласників у 2023 році перевищили 67 млрд доларів США з прогнозом зростання до 113 млрд доларів до 2027 року, причому найбільш руйнівним є піратство прямих спортивних трансляцій. Традиційні засоби захисту — контроль доступу, шифрування AES, системи DRM — виявляються безсилими проти інсайдерської загрози, коли пірат виступає легальним клієнтом і здійснює захоплення екрана після дешифрування контенту через так звану «аналогову діру». Це робить актуальною розробку альтернативних підходів, здатних ідентифікувати та нейтралізувати джерело витоку безпосередньо у відеопотоці протягом перших хвилин ефіру.
Мета роботи- підвищити захищеність контенту комерційних прямих трансляцій.
Об'єкт дослідження є процес захисту відеоданих від незаконної редистрибуції під час потокового передавання в реальному часі.
Предметом дослідження є система захисту контенту комерційних прямих трансляцій.
Методами дослідження математичне моделювання процесу ідентифікації порушника, методи теорії пошуку та оптимізації (метод дихотомії, золотого перерізу, Фібоначчі), а також методи цифрової обробки сигналів і комп'ютерного зору (частотна фільтрація, перетворення Хафа). Застосовано натурно-математичне моделювання запропонованого методу на даних реальної комерційної трансляції з оцінкою ефективності у порівнянні з традиційною

моделлю реактивного блокування. Запропонований метод активного трасування на основі динамічної дихотомії дозволяє автоматизувати процес виявлення джерела витоку, усунути залежність від реакції сторонніх платформ та значно скоротити час нейтралізації порушника. За результатами моделювання встановлено, що розроблений метод за час, пропорційний $\log_2 N$, забезпечує ідентифікацію всіх ≈ 2 000 джерел витоку для аудиторії 1,5 млн глядачів за 21 ітерацію (≈ 84 секунди), а коефіцієнт ефективності блокування зріс з 0,40 у традиційній моделі до 1,00 у запропонованому методі. Зокрема, метод не покладає додаткового обчислювального навантаження на кінцеві пристрої користувачів та інтегрується у наявну інфраструктуру OTT-провайдера без її докорінної перебудови.

Ключові слова: ПРЯМІ ТРАНСЛЯЦІЇ, ЦИФРОВИЙ МЕДІАКОНТЕНТ, OTT, ФОРЕНЗИЧНЕ МАРКУВАННЯ, АКТИВНЕ ТРАСУВАННЯ, ДИНАМІЧНА ДИХОТОМІЯ, КОНТРОЛЬНА ЗАВАДА, DRM, ІНФОРМАЦІЙНА БЕЗПЕКА, ВІДЕОПІРАТСТВО.

ABSTRACT

Diploma thesis "Modified Content Protection System for Commercial Live Broadcasts" contains 54 pages of text, 9 figures and 5 tables, and references 25 literary sources.

Relevance of the topic: protecting digital media content in commercial live broadcasts is a key aspect of preserving the economic model of OTT providers and rights holders, which determines the resilience of the entire streaming industry. Amid the rapid growth of illegal content redistribution, global financial losses for rights holders in 2023 exceeded $67 billion USD, with projections reaching $113 billion by 2027, with live sports piracy being the most damaging form. Traditional protection measures — access control, AES encryption, DRM systems — prove powerless against the insider threat, where a pirate acts as a legitimate subscriber and performs screen capture after content decryption through the so-called "analog hole." This makes it urgent to develop alternative approaches capable of identifying and neutralizing the leakage source directly within the video stream during the first minutes of broadcast.

The objective of the thesis is to enhance the security of content in commercial live broadcasts.

The object of research is the process of protecting video data from illegal redistribution during real-time streaming.

The subject of research is the content protection system for commercial live broadcasts.

Research methods include mathematical modeling of the violator identification process, methods from search and optimization theory (bisection method, golden section, Fibonacci search), as well as digital signal processing and computer vision techniques (frequency filtering, Hough transform). Natural-mathematical modeling of

the proposed method was applied to real commercial broadcast data, with effectiveness evaluated against the traditional reactive blocking model.

The proposed active tracing method based on dynamic bisection enables automated detection of the leakage source, eliminates dependence on third-party platform response, and significantly reduces the time required to neutralize the violator. Simulation results show that the developed method, operating in time proportional to $\log_2 N$, identifies all approximately 2,000 leakage sources within an audience of 1.5 million viewers in 21 iterations (approximately 84 seconds), while the blocking efficiency coefficient increased from 0.40 in the traditional model to 1.00 in the proposed method. Notably, the method places no additional computational load on end-user devices and integrates into the existing OTT provider infrastructure without requiring its fundamental restructuring.

Keywords: LIVE BROADCASTS, DIGITAL MEDIA CONTENT, OTT, FORENSIC WATERMARKING, ACTIVE TRACING, DYNAMIC BISECTION, CONTROL INTERFERENCE, DRM, INFORMATION SECURITY, VIDEO PIRACY.

ЗМІСТ

СПИСОК ТЕРМІНІВ І СКОРОЧЕНЬ

ABR — адаптивне потокове передавання (Adaptive Bitrate Streaming)

AES — симетричний блоковий шифр (Advanced Encryption Standard)

CDM — модуль дешифрування контенту (Content Decryption Module)

CDN — мережа доставки контенту (Content Delivery Network)

CENC — загальне шифрування (Common Encryption)

DASH — динамічне адаптивне потокове передавання через HTTP

DCT — дискретне косинусне перетворення

DMCA — Закон про авторське право у цифрову епоху (США)

DRM — управління цифровими правами (Digital Rights Management)

HLS — потокове передавання через HTTP (HTTP Live Streaming)

OTT — надання контенту поверх мережі оператора (Over-the-Top)

PPV — оплата за перегляд (Pay-Per-View)

QoE — якість сприйняття (Quality of Experience)

YUV — колірна модель «яскравість — кольоровість»

ВСТУП

Цифровий медіаринок сьогодні визначається стрімкою експансією технологій потокового передавання у реальному часі. Сегмент прямих трансляцій (Live Streaming) утримує понад 60 % сукупного обсягу відеостриму. Паралельно з розвитком легальних сервісів стрімко зростають і масштаби відеопіратства. За даними аналітичних звітів, у 2023 році глобальні втрати правовласників перевищили 67 млрд доларів США, а до 2027 року прогнозується їхнє зростання до 113 млрд. [23, 24]

Показовий приклад — серія боксерських поєдинків за звання абсолютного чемпіона світу між Олександром Усиком і Тайсоном Ф'юрі. За оцінками Yield Sec, лише одну подію з цієї серії нелегально подивилися щонайменше 20 мільйонів користувачів; втрати мовників перевищили 100 млн доларів. [22] Цифри красномовно свідчать: проблема не теоретична, а гостро практична.

Головні слабкі місця галузі — це «аналогова діра» (Analog Hole) та незаконна редистрибуція (Restreaming). Шифрування та DRM закривають канал передачі, але стають безсилими в момент, коли контент дешифрується у буфері кадру пристрою. Саме там зловмисник перехоплює чистий сигнал засобами захоплення екрана і миттєво пускає його неавторизованій аудиторії. Отже, методи, які дозволяють знайти джерело витоку безпосередньо у самому відеопотоці, є критично важливим напрямом захисту комерційних інтересів OTT-провайдерів.

Мета і завдання дослідження

Мета роботи — підвищити захищеність контенту комерційних прямих трансляцій.

Для досягнення поставленої мети визначено такі завдання:

1. Проаналізувати процес і проблематику захисту комерційних прямих трансляцій;
2. Проаналізувати наявні методи захисту контенту та їх обмеження;

3. Модифікувати систему захисту комерційних трансляцій шляхом застосування методу активного ітеративного трасування на основі динамічної дихотомії (методу контрольної завади) на стороні сервера;
4. Оцінити ефективність запропонованого рішення на прикладі реальної трансляції.

Об'єкт дослідження — процес захисту відеоданих від незаконної редистрибуції під час потокового передавання в реальному часі.

Предмет дослідження — система захисту контенту комерційних прямих трансляцій.

Методи дослідження — системний аналіз предметної області; математичне моделювання; методи теорії пошуку та оптимізації (метод дихотомії, золотого перерізу, Фібоначчі); методи цифрової обробки сигналів і комп'ютерного зору (частотна фільтрація, перетворення Хафа).

Наукова новизна. Модифіковано систему захисту комерційних прямих трансляцій шляхом інтеграції серверного маркування зображення з алгоритмом логарифмічного бінарного пошуку, що, на відміну від існуючих методів, дозволяє ідентифікувати пірата-інсайдера в реальному часі без збільшення обчислювального навантаження на клієнтський пристрій.
Практичне значення. Запропоноване рішення може бути комерціалізоване власниками хостингів прямих трянсляцій та CDN-мереж, що дозволить їм автоматично блокувати нелегальні ретрансляції за лічені хвилини, мінімізуючи фінансові втрати.

РОЗДІЛ 1 ПРОЦЕС ТА СТРУКТУРА ОНЛАЙН-ТРАНСЛЯЦІЇ

Щоб розібратися із загрозами та засобами захисту прямих трансляцій, спершу потрібно докладно зрозуміти сам технологічний ланцюг — як цифровий контент проходить шлях від камери до екрана глядача. Кожна ланка цього ланцюга має власні вразливості, а точки впровадження засобів безпеки задаються саме його структурою. Інтернет-мовлення сьогодні працює зовсім не так, як класичне ефірне телебачення: тут немає неперервного потоку, натомість використовується фрагментована модель доставки даних через HTTP.

1.1. Загальна архітектура системи потокового передавання

Сучасна технологія доставки комерційного контенту базується на принципі адаптивного потокового передавання (Adaptive Bitrate Streaming — ABR). Процес не є лінійним, а складається з низки послідовних етапів обробки на стороні сервера та реконструкції на стороні клієнта. Узагальнено ланцюг доставки містить такі ланки: джерело сигналу (Source), кодувальник (Encoder), транскодер та пакувальник (Transcoder/Packager), джерело контенту (Origin), мережу доставки контенту (CDN) та клієнтський відеоплеєр (Player).

Кожна з цих ланок виконує строго визначену функцію. Джерело формує первинний нестиснений відеопотік; кодувальник стискає його до прийнятного обсягу; транскодер створює кілька варіантів якості; пакувальник розбиває контент на дрібні фрагменти й супроводжує їх описовими файлами; точка походження зберігає підготовлений контент; CDN розподіляє його географічно ближче до користувача; нарешті, плеєр реконструює безперервне відео з окремих фрагментів. Така архітектура забезпечує масштабованість на мільйони одночасних глядачів, проте водночас породжує специфічні вразливості, детально розглянуті у розділі 2.

1.2. Кодування, транскодування та сегментація

Процес починається з джерела (професійна камера, мікшерний пульт, програмне середовище), що передає нестиснений (raw) відеопотік. Обсяг raw 4K при 60 кадрах/с — кілька гігабіт за секунду, передавати таке Інтернетом

неможливо. Тому сигнал надходить на кодувальник, який стискає його за стандартами H.264 (Advanced Video Coding), H.265 (HEVC) [11, 12] або AV1. Алгоритми усувають просторову та часову надлишковість через дискретне косинусне перетворення, передбачення руху, квантування коефіцієнтів — обсяг зменшується у десятки разів. Важлива властивість стиснення з втратами: воно безповоротно змінює значення пікселів. Звідси вимога до форензичного маркера — стійкість до повторного стиснення (перекодування), яке неминуче застосовує пірат при ретрансляції.

Оскільки глядачі підключаються з різних пристроїв за різної якості мережі, застосовується транскодування — формування з єдиного входу кількох варіантів якості, що утворюють «бітрейтну драбину» (240p, 360p, 480p, 720p, 1080p, 4K). Кожен варіант розбивається на короткі сегменти (зазвичай 2–10 с); межі сегментів різних якостей вирівняні, що дозволяє плеєру безшовно перемикатися між ними. Пакувальник формує описовий файл — маніфест (HLS) або MPD (DASH). Саме етап пакування — природне місце впровадження серверного захисту: тут контент шифрується, додаються метадані ліцензування, тут же розташовується маніпулятор плейлистів.

1.3. Протоколи доставки HLS і DASH; адаптація

Фрагментований контент доставляється через HTTP двома протоколами. HLS (HTTP Live Streaming, Apple) [10] використовує текстові плейлисти M3U8 і фрагментований формат CMAF. DASH (Dynamic Adaptive Streaming over HTTP, ISO/IEC) [9] незалежний від кодеків, описує контент через XML-файл MPD. Обидва реалізують одну ідею: клієнт завантажує описовий файл, аналізує доступні якості, послідовно запитує сегменти HTTP-запитами. Стандартний HTTP дає кешування проміжними вузлами і доставку через звичайний CDN. Конвергенція навколо CMAF дозволяє використовувати ті ж самі медіафайли одночасно для HLS та DASH.

Центральний механізм ABR — алгоритм адаптації на клієнті. Плеєр оцінює стан каналу і рівень буфера, для кожного наступного сегмента обирає

таку якість, яку гарантовано завантажить вчасно. Для запропонованого методу принципово, що адресація запитів повністю контролюється провайдером через зміст маніфесту: сервер може динамічно для окремого користувача чи групи підмінити адреси сегментів — спрямувати одних на «чисті», інших на марковані. Підміна абсолютно прозора для глядача і не порушує безперервності відтворення.

1.4. CDN, затримка та місце модулів захисту

Мережа доставки контенту (CDN) — це географічно розподілена система кеш-серверів (Edge), що розвантажує точку походження і скорочує мережеву затримку. Під час масових подій навантаження на CDN сягає піків. Наскрізна затримка прямих трансляцій (glass-to-glass) складається із затримок кодування, пакування, мережі та буферизації плеєра. Класичний HLS — 20–40 с, що неприйнятно для інтерактиву. [18] З'явилися Low-Latency HLS і LL-DASH (затримка 2–5 с за рахунок передачі сегментів частинами), а також WebRTC для наднизьких затримок. Тривалість однієї ітерації трасування безпосередньо залежить від тривалості сегмента.

Аналіз архітектури дає оптимальні точки впровадження захисту: шифрування та управління ключами — на пакуванні і сервері ліцензій; контроль доступу — на рівні видачі маніфесту; форензичне маркування — на серверній стороні, у складі пакувальника та маніпулятора плейлистів. На рис. 1.1 наведено структурну схему модифікованої системи захисту, де до стандартного пайплайну інтегровано модуль накладання водяних знаків та модуль активного трасування. Ключово: ці модулі працюють на сервері й не додають навантаження на кінцевий пристрій.

Рисунок 1.1 — Структурна схема модифікованої системи захисту комерційних прямих трансляцій.

Висновки до розділу 1

Простежено технологічний ланцюг доставки прямої трансляції від камери до плеєра глядача. Фрагментована HTTP-архітектура HLS/DASH дає провайдеру повний контроль над маніфестами та адресним наданням сегментів окремим групам — саме це робить можливим запропонований метод трасування.

РОЗДІЛ 2 ІСНУЮЧІ ПРОБЛЕМИ ТРАНСЛЯЦІЙ

Архітектура потокового передавання масштабована та гнучка, але вразливостей у ній вистачає. Походять вони з різних джерел: одні випливають із самої необхідності показати відео людині, інші — з обмежень криптографії, ще інші — з економіки розповсюдження контенту. Далі розглянемо чотири ключові проблеми галузі та сформулюємо узагальнену модель загроз, з якої безпосередньо випливають вимоги до системи захисту.

2.1. «Аналогова діра» (Analog Hole) та захоплення екрана

Фундаментальною проблемою будь-якої системи захисту медіаконтенту є необхідність його кінцевого відтворення для сприйняття людиною. Хоч би яким надійним було наскрізне шифрування, у певний момент відео має бути дешифроване та виведене на екран у формі, придатній для зорового сприйняття. Цей момент і утворює так звану «аналогову діру» — принципову вразливість, яку неможливо усунути суто криптографічними засобами.

У момент виведення зображення контент залишає захищене апаратне середовище (наприклад, ізольоване середовище виконання TrustZone або захищений відеоконвеєр) і потрапляє у буфер кадру операційної системи у відкритому вигляді. Саме на цьому етапі зловмисник, що має легальний доступ до трансляції, може здійснити перехоплення. Розрізняють два основні способи захоплення.

Програмне захоплення полягає у використанні спеціалізованого програмного забезпечення (OBS Studio, Bandicam, вбудовані засоби запису екрана), яке зчитує вміст буфера кадру або перехоплює виклики графічного інтерфейсу. Сучасні системи захисту намагаються протидіяти цьому через механізми захищеного відтворення, що роблять область відео «чорною» для засобів захоплення, проте ці механізми обходяться на пристроях зі зниженим рівнем апаратної безпеки.

Апаратне захоплення є значно складнішим для протидії: зловмисник використовує фізичні пристрої — HDMI-розгалужувачі та карти захоплення, які

перехоплюють відеосигнал на шляху до монітора. Хоча інтерфейс HDMI захищений технологією HDCP, на ринку широко доступні пристрої, що знімають цей захист (HDCP-strippers), після чого сигнал записується у первісній якості. Проти апаратного захоплення криптографія безсила в принципі.

Таким чином, «аналогова діра» зміщує акцент захисту з запобігання витоку (що неможливо гарантувати) на виявлення та ідентифікацію джерела витоку після його виникнення. Саме на цьому принципі ґрунтуються методи форензичного маркування та активного трасування, що становлять предмет цієї роботи.

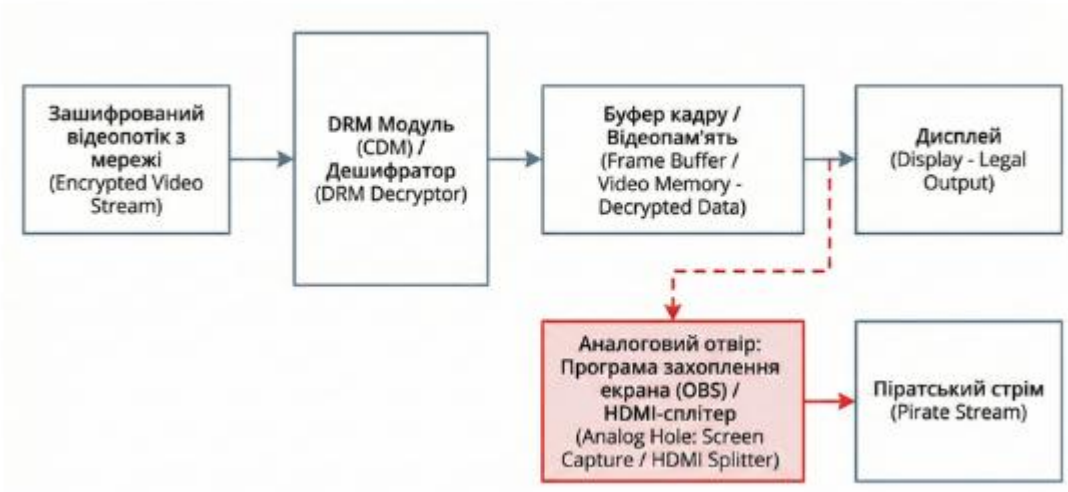

Рисунок 2.1 — Структурна схема виникнення вразливості «аналогового отвору» після дешифрування сигналу.

2.2. Вплив захисту на затримку (Latency) та якість сприйняття (QoE)

Упровадження багаторівневих систем захисту не є безкоштовним з погляду продуктивності. У комерційних прямих трансляціях, особливо спортивних та кіберспортивних подій, критичним параметром є затримка від моменту події до її відображення в глядача, а також відсутність перерв у відтворенні. Будь-яка додаткова обробка контенту — дешифрування, перевірка ліцензій, накладання маркерів — потенційно збільшує цю затримку та навантаження на пристрій.

Процес покадрового дешифрування високоякісного відео (4K чи 8K) у реальному часі створює суттєве навантаження на центральний та графічний процесори кінцевого пристрою. На потужних настільних системах це майже непомітно, проте на смарт-телевізорах, телевізійних приставках і мобільних пристроях, де обчислювальні ресурси обмежені, нестача потужності призводить до низки негативних явищ.

Якість сприйняття (Quality of Experience, QoE) [18] — це інтегральна суб'єктивно-об'єктивна характеристика, що відображає задоволеність користувача переглядом. Основними об'єктивними метриками QoE для адаптивного стрімінгу є: час початкової буферизації (startup delay) — затримка до початку відтворення; частка часу повторної буферизації (rebuffering ratio) — частка часу, протягом якого відтворення зупинялося; частота та тривалість зупинок (stalls); кількість перемикань якості; середня роздільна здатність відтворення. Дослідження показують, що навіть незначне зростання частки повторної буферизації [18, 19] різко знижує задоволеність користувачів та збільшує ймовірність припинення перегляду.

Виникає об'єктивний конфлікт інтересів: посилення захисту погіршує QoE, а спрощення захисту підвищує ризик піратства. Класичні клієнтські методи форензичного маркування додатково навантажують пристрій, оскільки вимагають обробки кожного кадру локально. Це є вагомим аргументом на користь перенесення функцій маркування та трасування на серверну сторону, що й реалізовано у запропонованому методі: кінцевий пристрій не виконує жодної додаткової обробки, а отже, QoE не погіршується.

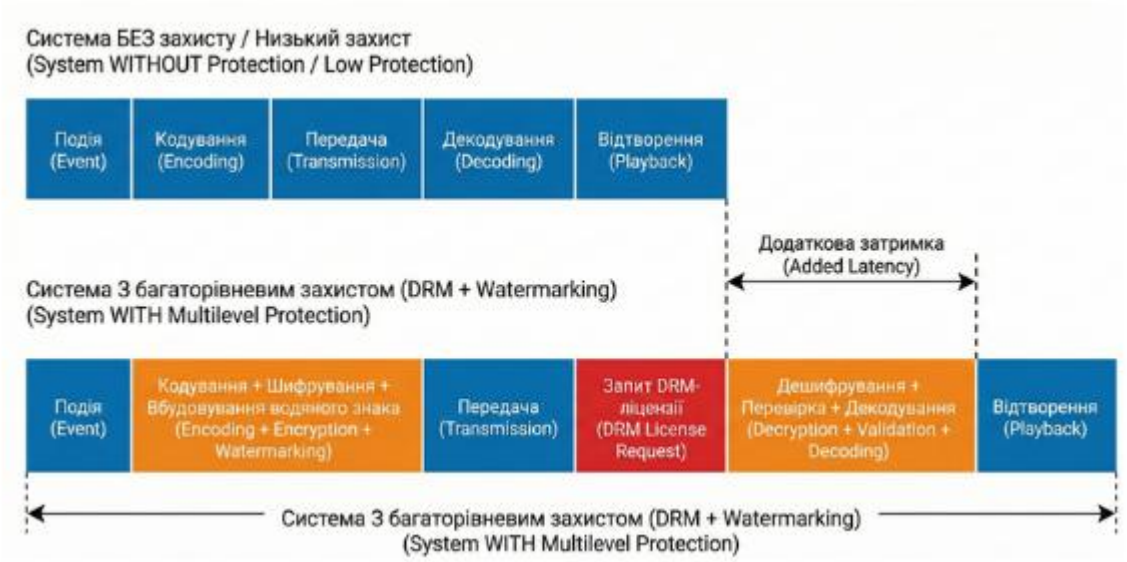

Рисунок 2.2 — .

2.3. Складність управління ключами (Key Management)

Архітектура захищеного стрімінгу вимагає, щоб кожен клієнтський пристрій для дешифрування контенту звернувся до сервера ліцензій і отримав ключ дешифрування разом із описом дозволених прав. Така централізована модель добре працює за помірного навантаження, проте під час масштабних Live-подій породжує гостру проблему масштабування.

Явище, відоме як «проблема шквального натовпу» (Thundering Herd Problem), виникає тоді, коли мільйони користувачів намагаються підключитися до трансляції майже одночасно — наприклад, безпосередньо перед початком фінального поєдинку чи вирішального матчу. У цей короткий проміжок часу сервер ліцензій отримує лавиноподібний потік запитів на видачу ключів, що за характером навантаження нагадує розподілену атаку на відмову в обслуговуванні (DDoS). Пікова інтенсивність може у десятки разів перевищувати середню.

Якщо інфраструктура видачі ліцензій не розрахована на такий пік, легальні користувачі, які оплатили доступ, стикаються з відмовами, тривалими очікуваннями та неможливістю розпочати перегляд саме в найважливіший момент. Це призводить до прямих репутаційних та фінансових втрат, а також, парадоксально, штовхає частину розчарованих легальних користувачів до

пошуку піратських трансляцій, які в цей момент уже доступні. Для пом'якшення проблеми застосовують попереднє кешування ліцензій, горизонтальне масштабування серверів ліцензій, черги запитів та механізми обмеження інтенсивності, проте повністю усунути ризик складно.

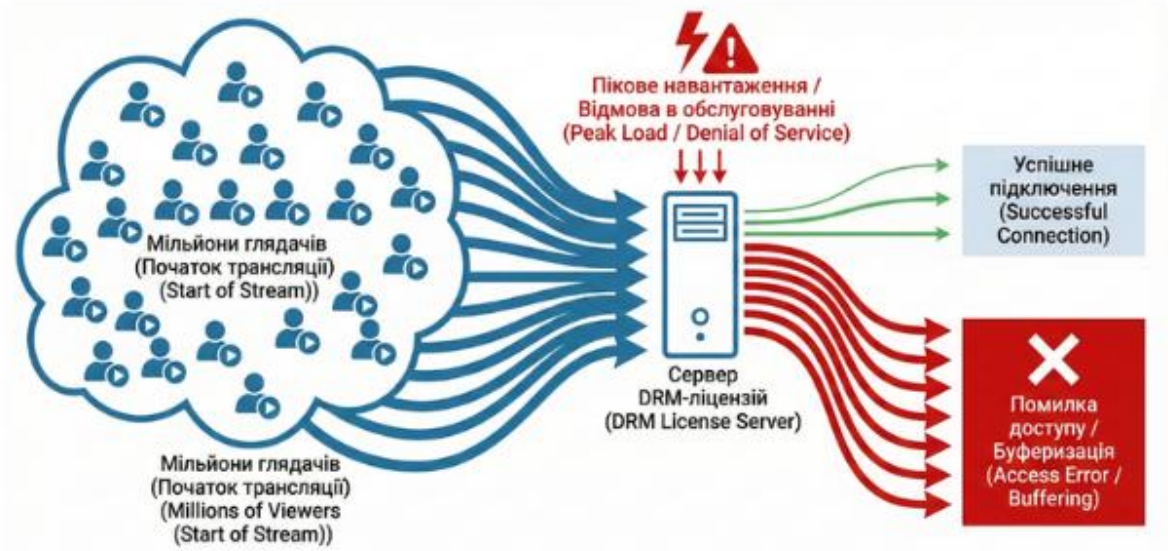

Рисунок 2.3 — Схема виникнення проблеми «шквального натовпу» на сервері ліцензій під час початку масової трансляції.

2.4. Незаконна редистрибуція (Restreaming)

Найбільш фінансово руйнівною загрозою для комерційних платформ є незаконна редистрибуція — процес, за якого авторизований користувач, що має легальну підписку, зловживає своїм доступом. Він використовує власне обладнання для перехоплення розшифрованого потоку (через «аналогову діру») та його миттєвої повторної трансляції на широку аудиторію через сторонні платформи: відеохостинги, стрімінгові сервіси, канали месенджерів, спеціалізовані піратські сайти та IPTV-сервіси. [23, 24]

Фундаментальна проблема полягає у критичній асиметрії доступу, яку зручно описати моделлю «один-до-багатьох»: одна-єдина легально оплачена ліцензія може слугувати джерелом безкоштовного перегляду для тисяч або навіть десятків тисяч неавторизованих користувачів. Як показано у прикладі розділу 6, на одну піратську трансляцію в середньому припадало близько десяти тисяч глядачів. Така асиметрія робить піратство економічно надзвичайно

привабливим: витрати зловмисника обмежуються вартістю однієї підписки, тоді як завдані правовласнику збитки на порядки більші.

Доцільно розрізняти кілька типів джерел витоку за мотивацією та масштабом. Випадковий пірат ретранслює подію для невеликого кола (друзі, спільнота) без систематичної комерційної мети. Комерційний пірат організовує платні або рекламно монетизовані трансляції, інколи з власною інфраструктурою перекодування та кількома резервними каналами. Найскладнішими є організовані IPTV-оператори, що агрегують десятки каналів і використовують професійні засоби стійкості — резервні джерела, автоматичне перемикання, видалення видимих логотипів. Запропонований метод спрямований насамперед проти джерела сигналу, а не проти кінцевої платформи, що робить його ефективним незалежно від типу пірата.

Ключова безпорадність традиційних систем полягає в тому, що на етапі підключення пірат технічно не відрізняється від чесного користувача: він має валідну підписку, валідний токен і валідну ліцензію. Системи контролю доступу не мають жодних формальних підстав відмовити йому. Витік відбувається вже після дешифрування, поза контролем криптографічних механізмів. Отже, єдиним способом протидії є вбудовування у сам відеопотік прихованої інформації, що дозволяє згодом ідентифікувати, з якого саме облікового запису відбувся витік.

Рисунок 2.4 — Модель незаконної редистрибуції контенту «один-до-багатьох» через легальний обліковий запис.

2.5. Узагальнена модель загроз

Для коректного формулювання вимог до системи захисту доцільно узагальнити розглянуті вразливості у вигляді моделі загроз, що описує можливості та обмеження зловмисника. У межах цієї роботи приймається модель внутрішнього порушника (insider threat) з такими характеристиками.

- **Легальний доступ.** Порушник має дійсну підписку, проходить автентифікацію та отримує валідну ліцензію на дешифрування. Він не атакує криптографію безпосередньо, а зловживає легітимним доступом.
- **Можливість захоплення.** Порушник здатний отримати дешифрований відеопотік через програмне або апаратне захоплення екрана, оминаючи захист відтворення.
- **Можливість перекодування.** Перед ретрансляцією порушник застосовує повторне стиснення, може змінювати роздільну здатність, обрізати краї кадру, накладати власні елементи інтерфейсу. Це створює вимогу стійкості (robustness) маркера.
- **Затримка ретрансляції.** Піратський канал має власну затримку (буферизація, перекодування), що впливає на час замкнення циклу зворотного зв'язку та враховується при оцінці швидкодії.
- **Можливість змови.** У розширеній моделі кілька порушників можуть кооперуватися, порівнюючи копії та комбінуючи фрагменти, що формує вимогу стійкості до атак змови (collusion).

Висновки до розділу 2

Класичні засоби — контроль доступу, шифрування, паролі — не працюють проти інсайдера: піратом є сам легальний клієнт, а витік відбувається після дешифрування. «Аналогову діру» закрити неможливо, тож логіка захисту має змінитися — не запобігати, а швидко знаходити джерело у відеопотоці. Із побудованої моделі загроз постають вимоги: серверна реалізація без навантаження на клієнт, стійкість маркера до перекодування, висока швидкодія.

РОЗДІЛ 3 ОГЛЯД ТА АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ЗАХИСТУ МЕДІАКОНТЕНТУ

Захист комерційного відеоконтенту будується ешелоновано. Жоден окремий рівень не вирішує задачі сам по собі, проте їх сукупність робить атаку дорогою і складною для зловмисника. У літературі прийнято виділяти чотири основні рівні: контроль доступу, криптографічний захист, DRM та цифрові водяні знаки. Окремо коротко розглянемо теорію динамічного трасування зрадників — вона є концептуальним підґрунтям для методу, запропонованого у наступному розділі.

3.1. Контроль доступу та автентифікація

Першим рубежем захисту є перевірка легітимності користувача перед наданням доступу до контенту. Сучасні системи спираються на токенну автентифікацію замість передавання облікових даних у кожному запиті. Після успішного входу сервер видає користувачеві підписаний токен (наприклад, у форматі JWT — JSON Web Token), що містить ідентифікатор сесії, перелік прав та термін дії, засвідчені криптографічним підписом.

Для захисту самих посилань на контент застосовують підписані URL-адреси (signed URL) з обмеженим терміном дії: сервер генерує код автентифікації повідомлення (Message Authentication Code, MAC) на основі секретного ключа, шляху до ресурсу та часу закінчення дії, додаючи його до адреси. Edge-сервер CDN перевіряє цей код і відмовляє у видачі, якщо посилання прострочене або підроблене. Це унеможливлює просте копіювання посилань.

Додатковими механізмами контролю доступу є географічне обмеження (geo-blocking) на основі IP-адреси, обмеження кількості одночасних сесій на один обліковий запис (concurrency control) та аналіз поведінкових аномалій. Проте всі ці механізми мають спільне принципове обмеження, окреслене у розділі 2: вони контролюють вхід у систему, але безсилі проти зловживання вже

наданим легальним доступом. Внутрішній порушник долає цей рівень тривіально, оскільки є легітимним користувачем.

3.2. Криптографічний захист відеопотоку

Основою конфіденційності контенту під час зберігання та передавання є симетричне блокове шифрування за стандартом AES (Advanced Encryption Standard) [14, 15] з довжиною ключа 128 або 256 біт. Кожен медіасегмент шифрується перед розміщенням на CDN, тож навіть у разі перехоплення трафіку зашифрований сегмент є непридатним для відтворення без ключа.

Застосовуються різні режими роботи шифру. Режим CBC (Cipher Block Chaining) ланцюжково зв'язує блоки, тоді як режим CTR (Counter) перетворює блоковий шифр на потоковий і дозволяє паралельне дешифрування, що зручно для відео. Для забезпечення сумісності між різними системами DRM розроблено стандарт загального шифрування CENC (Common Encryption, ISO/IEC 23001-7) [8]: контент шифрується один раз, а різні системи DRM використовують власні механізми лише для захищеного передавання спільного ключа. У межах CENC застосовують схеми повного шифрування зразка (cenc) та шифрування з пропусками (cbcs), що шифрують лише частину байтів, знижуючи обчислювальне навантаження.

Окремою інженерною задачею є ротація ключів — періодична зміна ключа дешифрування протягом трансляції, що обмежує наслідки компрометації окремого ключа. Проте, як і у випадку контролю доступу, криптографія захищає виключно канал та сховище: щойно легальний клієнт отримує ключ і дешифрує контент для відтворення, захист завершується, і набуває чинності проблема «аналогової діри».

3.3. Системи управління цифровими правами (DRM)

Самого лише шифрування недостатньо, оскільки ключ дешифрування потрібно безпечно доставити на пристрій користувача й гарантувати, що він не буде вилучений та використаний поза дозволеними межами. Цю задачу розв'язують системи управління цифровими правами. Архітектура DRM

відокремлює зашифрований контент від ліцензії: контент вільно розповсюджується через CDN, а ключі та правила використання передаються окремим захищеним каналом до спеціального модуля дешифрування контенту (Content Decryption Module, CDM) на пристрої клієнта.

На ринку домінують три екосистеми DRM: Widevine (Google), PlayReady (Microsoft) та FairPlay (Apple), кожна з яких підтримується відповідними платформами та браузерами. Для охоплення всіх пристроїв провайдери застосовують стратегію кількох DRM (multi-DRM), упаковуючи контент за стандартом CENC та видаючи ліцензії через відповідну систему залежно від пристрою. Взаємодія браузера із CDM стандартизована специфікацією Encrypted Media Extensions (EME) консорціуму W3C. [13]

Важливою характеристикою DRM є рівень захищеності (security level): найвищий передбачає виконання дешифрування у захищеному апаратному середовищі (TrustZone), нижчі — програмну ізоляцію. Високоякісний контент (4K) видається лише пристроям із апаратним рівнем. Попри це, DRM не усуває «аналогову діру»: на пристроях нижчого рівня або при апаратному захопленні сигнал перехоплюється. Крім того, саме DRM породжує проблему «шквального натовпу». Втім, у запропонованому методі DRM відіграє ключову роль на завершальному етапі — через API відкликання ліцензії скомпрометований акаунт миттєво позбавляється доступу.

3.4. Цифрові водяні знаки та форензичне маркування

На відміну від попередніх рівнів, що намагаються запобігти витоку, цифрові водяні знаки (digital watermarking) спрямовані на виявлення джерела витоку [1, 3, 4] після його виникнення. Метод полягає у вбудовуванні у відеосигнал прихованої інформації — непомітних для глядача змін, що кодують ідентифікатор користувача або сесії. Якщо контент згодом виявляється у нелегальному обігу, аналіз вбудованого знака дозволяє встановити джерело.

Водяні знаки класифікують за кількома ознаками. За областю вбудовування розрізняють методи просторової області, що змінюють

безпосередньо значення пікселів, та методи частотної області, що модифікують коефіцієнти перетворень (дискретного косинусного DCT чи дискретного вейвлет-перетворення DWT); останні зазвичай стійкіші до стиснення. За призначенням розрізняють крихкі знаки (fragile), що руйнуються за найменшої зміни й служать для перевірки цілісності, та робастні знаки (robust), що мають витримувати перекодування, масштабування та інші перетворення. Для завдання протидії піратству потрібні саме робастні форензичні знаки.

Принципово важливим є місце вбудовування. Клієнтське маркування дає унікальність ідентифікатора, але навантажує пристрій користувача та вимагає захисту самого процесу маркування. [17, 21] Серверне виконується інфраструктурою провайдера: один із його різновидів — варіативна доставка сегментів, коли для кожного фрагмента готується кілька варіантів і користувач отримує індивідуальну послідовність. Саме серверний підхід покладено в основу запропонованого методу, проте, на відміну від класичної пасивної схеми, він застосовується для активного зондування (див. розділ 4).

Окрему категорію становлять видимі маркери — напівпрозорі ідентифікатори чи коди, накладені поверх зображення. Вони надзвичайно точні для остаточної верифікації, проте погіршують перегляд і легко видаляються обрізанням, тому застосовуються вибірково. У запропонованому методі видимий маркер (Сегмент C) використовується лише одноразово, на завершальному етапі верифікації вже локалізованого підозрюваного.

3.5. Динамічне трасування зрадників і стійкість до змови

Теоретичною основою форензичного маркування є концепція трасування зрадників (traitor tracing), що виникла у криптографії широкомовного шифрування [2, 5]. Завдання формулюється так: розповсюдити контент серед множини користувачів у такий спосіб, щоб за будь-якою нелегальною копією можна було встановити, який саме користувач (або які користувачі) став джерелом витоку.

Розрізняють статичне та динамічне трасування. У статичних схемах кожному користувачеві призначається фіксований кодовий набір ще до розповсюдження, і джерело встановлюється постфактум за аналізом перехопленої копії. У динамічних схемах, запропонованих у роботах Фіата і Тасси [5], маркування адаптивно змінюється в часі залежно від спостережуваної піратської копії, що дозволяє звужувати коло підозрюваних безпосередньо під час трансляції. Саме динамічний підхід природно відповідає сценарію прямих трансляцій і є концептуальною основою запропонованого методу.

Найскладніша теоретична проблема — атаки змови (collusion). Кілька порушників, об'єднавши копії, можуть сформувати «усереднену» версію, в якій індивідуальні маркери частково знищені. Для протидії існують стійкі до змови коди: Боне–Шоу гарантують виявлення хоча б одного учасника коаліції обмеженого розміру ціною подовження кодового слова [6]; ймовірнісні коди Тардоса асимптотично оптимальні і застосовуються у промислових системах [7]. Інтеграція таких кодів — природний напрям посилення методу, базова бінарна модель якого розрахована на одиничне некооперативне джерело.

Узагальнене порівняння розглянутих методів захисту за принципом дії, перевагами та вразливостями наведено в таблиці 3.1.

Таблиця 3.1 — Порівняння методів захисту медіаконтенту

Метод	**Принцип роботи**	**Переваги**	**Недоліки / вразливості**
Контроль доступу (токени)	Перевірка підписаних токенів та URL із MAC.	Простота, відсіювання неавторизованих запитів.	Безсилий проти інсайдера — легального клієнта.
Шифрування (AES, CENC)	Симетричне шифрування сегментів (AES-128/256).	Надійна конфіденційність каналу та сховища.	«Аналогова діра» після дешифрування у буфер кадру.

Метод	Принцип роботи	Переваги	Недоліки / вразливості
DRM (multi-DRM)	Відокремлення контенту від ліцензії; CDM, рівні захисту.	Безпечна доставка ключів, апаратна ізоляція.	Затримка, навантаження, «шквальний натовп», не усуває витік.
Традиційні (клієнтські) водяні знаки	Вбудовування ідентифікатора у потік на пристрої.	Залишається у потоці після дешифрування.	Високе навантаження на клієнт, ризик втручання.
Модифікована система (активне трасування)	Ітеративний поділ аудиторії та ідентифікація за появою завади на стрімі.	Серверна реалізація, висока швидкодія, без навантаження на клієнт.	Потребує інтеграції модулів на CDN; базово чутлива до змови.

Висновки до розділу 3

Контроль доступу, шифрування та DRM добре закривають канал передачі та сховище, але не вирішують проблеми інсайдерської редистрибуції після дешифрування. Серед різновидів форензичного маркування динамічне трасування зрадників найкраще підходить для прямих трансляцій, проте класичні пасивні схеми надто повільні для Live. Логічним кроком є активна серверна схема трасування з мінімальним навантаженням на клієнт.

РОЗДІЛ 4 МЕТОД АКТИВНОГО ТРАСУВАННЯ НА ОСНОВІ ДИНАМІЧНОЇ ДИХОТОМІЇ

Далі викладається сутність запропонованого методу: від базової ідеї до формального опису та обґрунтування. Метод націлений на головну ваду класичних схем форензичного маркування — повільне накопичення інформації під час пасивного спостереження за піратською копією. Замість цього система переходить до активної взаємодії з джерелом витоку у реальному часі.

4.1. Концепція активного трасування та метод «контрольної завади»

Більшість сучасних систем форензичного маркування побудована за пасивною схемою. Кожному користувачеві при підключенні присвоюється унікальна заздалегідь визначена послідовність маркованих сегментів — свого роду «штрих-код». Щоб знайти пірата, систему перехоплює його стрім і поступово, фрагмент за фрагментом, зчитує цей код, а потім ще й аналізує постфактум. Для прямих трансляцій така схема працює погано: комерційна цінність події вичерпується за десятки хвилин, а пасивне зчитування коду триває довше.

Натомість у цій роботі стеганографічний знак використано не як заздалегідь зашитий ідентифікатор, а як динамічний зондувальний сигнал — **«контрольну заваду»**. Принципова відмінність: система **не зчитує жодної заздалегідь визначеної комбінації маркованих сегментів** на кшталт А–Б–А–Б. Замість цього вона реагує безпосередньо на сам факт, що завада з'явилась на екрані порушника саме на цій ітерації.

Між маніпулятором плейлистів на Edge CDN провайдера та модулем моніторингу, який у реальному часі аналізує піратський стрім, виникає замкнений цикл зворотного зв'язку. Система не чекає, поки увесь код «прокрутиться»; вона сама провокує появу маркованих сегментів у потоці порушника, маневрує групами підписників і спостерігає, чи з'явилася завада. Пасивне спостереження замінюється керованим звуженням кола підозрюваних.

Кожна ітерація тут максимально інформативна: один акт зондування дає рівно один біт інформації про положення порушника у множині підозрюваних — є завада чи немає. Звідси випливає теоретично мінімальна кількість кроків — логарифмічна складність пошуку. Більше того, рішення про блокування можна приймати ще до того, як повний цикл спостереження завершиться.

4.2. Модель загрози та базові припущення

Зафіксуємо припущення базового алгоритму (на основі моделі загроз із розділу 2): простір пошуку утворюють N активних легальних підключень, серед яких є джерело витоку; система моніторингу має доступ до перехопленого піратського стріму та надійно визначає наявність завади у кадрі; маніпулятор плейлистів прозоро підмінює адресу сегмента на марковану версію для будь-якої підмножини користувачів; розглядається одиничне некооперативне джерело (множинні джерела та змова — окремо у розділах 4.3 і 6.2). За цих припущень задача зводиться до класичного пошуку елемента у скінченній множині бінарними запитами — оптимально розв'язується методом дихотомії.

4.3. Математична модель алгоритму трасування

Ідентифікація реалізується у вигляді циклу з повторюваними кроками. При виявленні факту незаконної редистрибуції масив усіх активних легальних підключень N віртуально ділиться на дві рівні групи — А та Б. Маніпулятор плейлистів динамічно змінює маршрутизацію: Група А починає отримувати потік із вбудованою контрольною завадою, Група Б — оригінальний чистий потік. Екстрактор у реальному часі аналізує піратську трансляцію: якщо на ній фіксується завада — джерело у Групі А (Б відкидається), якщо стрім залишається чистим — порушник у Групі Б. Локалізована група знову ділиться навпіл, і так далі — простір пошуку зменшується вдвічі на кожному кроці.

Ще раз підкреслимо: ключовим сигналом є не зчитування накопиченого коду, а саме поява чи відсутність завади на конкретному кроці. Після і-ї ітерації кількість підозрюваних N / 2 у степені і, ізоляція досягається при значенні 1. Звідси максимальна кількість ітерацій I та загальний час трасування T:

$$I = \lceil \log_2 N \rceil$$

$$T\_дет = I \cdot T\_сег = (\log_2 N) \cdot T\_сег$$

де T_сег — тривалість одного медіасегмента. Логарифмічна залежність означає, що навіть багатократне зростання аудиторії додає лише кілька ітерацій: подвоєння N — рівно одну.

Практичний розрахунок. Для N = 1 200 000 і T_сег = 4 с потрібно $\lceil \log_2 1\,200\,000 \rceil = 21$ ітерацію, час трасування $21 \cdot 4 = 84$ секунди. Метод нейтралізує витік ще на ранніх етапах трансляції (детально у розділі 6).

За умови безпомилкового розпізнавання завади ймовірність правильної локалізації прямує до одиниці. Накопичення помилок мінімізує завершальний етап верифікації видимим маркером (підрозділ 5.6) — він дає остаточне підтвердження перед блокуванням.

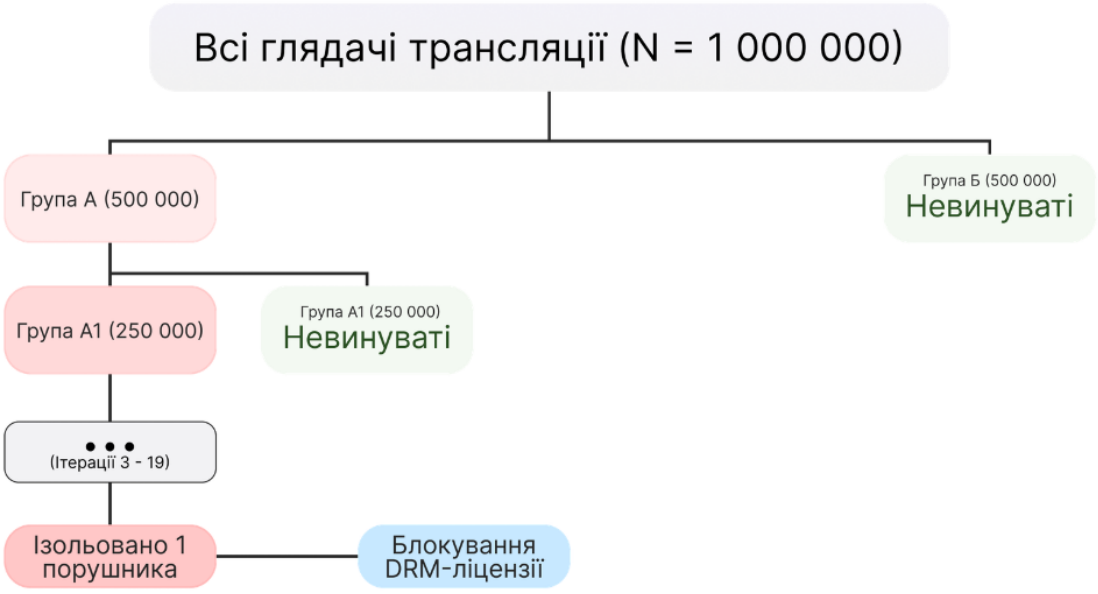

Рисунок 4.1 — Дерево пошуку (дихотомія) для ізоляції джерела витоку.

4.4. Порівняльний аналіз математичних стратегій ідентифікації

Хоча дихотомія є інтуїтивно очевидним вибором, для обґрунтованого рішення необхідно порівняти її з іншими класичними методами теорії пошуку та оптимізації за критеріями швидкодії, обчислювальних витрат та придатності до динамічного Live-середовища. Розглянуто три стратегії.

Метод дихотомії (бінарний пошук)

Полягає у симетричному поділі множини підозрюваних на дві рівні частини у пропорції 50/50. Забезпечує найменшу можливу кількість ітерацій порядку $\log_2 N$ та найпростішу інфраструктурну реалізацію — потребує лише двох станів сегмента (з завадою та без неї), що рівномірно розподіляє навантаження на CDN і мінімізує обсяг додаткового кешу.

Основним недоліком методу є чутливість до атак змови. Якщо кілька порушників об'єднують свої копії, порівнюючи їх та ретранслюючи лише сегменти без завади або комбінуючи фрагменти різних копій, сувора бінарна логіка «є шум / немає шуму» може давати збій. Базова модель розрахована на одиничне некооперативне джерело; для протидії коаліціям метод потребує надбудови у вигляді стійких до змови кодів — зокрема ймовірнісних кодів Тардоса або кодів Боне–Шоу [6, 7], розглянутих у розділі 3.

Метод золотого перерізу (Golden Section Search)

Базується на асиметричному поділі інтервалу в ірраціональній пропорції золотого перерізу $\varphi \approx 1{,}618$ (приблизно 62 % на 38 %). Метод є еталонним для пошуку екстремумів неперервних унімодальних функцій, де він мінімізує кількість обчислень цільової функції завдяки повторному використанню точок. Однак для дискретної множини облікових записів така асиметрія дає надлишковість: у найгіршому випадку пошук триває приблизно на 14–16 % довше, ніж при дихотомії. Крім того, нерівномірний поділ ускладнює балансування навантаження на Edge-сервери, оскільки групи виходять різного розміру.

Метод Фібоначчі (Fibonacci Search)

Використовує числа Фібоначчі для визначення точок поділу й оперує винятково цілими числами, що формально зручно для підрахунку дискретних користувачів. Проте метод вимагає заздалегідь знати точну фіксовану кількість елементів та число ітерацій ще до початку пошуку. Для високодинамічної Live-аудиторії, у якій кількість підключень безперервно змінюється (глядачі

приєднуються та відключаються), ця вимога робить метод надто громіздким та практично незастосовним без постійного перерахунку.

Порівняння трьох стратегій за ключовими характеристиками наведено в таблиці 4.1.

Таблиця 4.1 — Порівняння стратегій ідентифікації порушника

Характеристика	**Дихотомія**	**Золотий переріз**	**Фібоначчі**
Складність пошуку	$\log_2 N$	$1{,}44 \cdot \log_2 N$	$\log_{1{,}618} N$
Швидкість (1 млн)	~20 кроків (80 с)	~25 кроків (100 с)	~23 кроки (92 с)
Гнучкість у Live	Висока	Низька	Дуже низька
Ресурси сервера	Мінімальні (2 потоки)	Середні (асиметричні)	Середні (залежать від N)

Для комерційних систем стрімінгу метод дихотомії є безальтернативним лідером: він гарантує найшвидшу та найстабільнішу ізоляцію порушника за мінімальних витрат обчислювальних ресурсів CDN і природно підтримує динамічну зміну розміру аудиторії.

4.5. Особливості масштабування алгоритму (k-арний пошук)

Теоретичний розвиток системи може базуватися на переході від бінарної логіки до k-арного дерева пошуку, що дозволяє прискорити виявлення завдяки одночасному поділу аудиторії на більшу кількість груп. У базовій моделі система оперує алфавітом із двох символів (k = 2: «чисто» / «завада»), що дає швидкість порядку $\log_2 N$. При використанні алфавіту з k символів (один чистий сегмент і $k-1$ сегментів із різними просторовими масками шуму) кожна ітерація надає $\log_2 k$ біт інформації, а складність зменшується до log_k N. Розрахунок необхідної кількості кроків для різних k наведено в таблиці 4.2.

Таблиця 4.2 — Кількість кроків для ідентифікації порушника залежно від масштабування алгоритму

Розмір алфавіту k	**100 000**	**500 000**	**1 000 000**	**3 000 000**
2 символи	17	19	20	22

Розмір алфавіту k	100 000	500 000	1 000 000	3 000 000
4 символи	9	10	10	11
8 символів	6	7	7	8
16 символів	5	5	5	6

Переваги масштабування. Кількість кроків стрімко падає: для 1 млн глядачів перехід від 2 до 16 символів зменшує число ітерацій з 20 до 5, тобто час виявлення скорочується з 80 до 20 секунд.

Недоліки масштабування. Реалізація k-арного пошуку вимагає кодування кожного сегмента у k варіаціях, що збільшує навантаження на транскодер та підвищує вимоги до дискового кешу CDN приблизно у k разів. Крім того, ускладнюється аналіз завад: екстрактор має безпомилково розпізнавати, який саме з k−1 видів шуму присутній у перетисненому стрімі, що підвищує ризик хибних спрацьовувань (False Positives).

Обґрунтування вибору бінарної моделі. У межах цієї роботи для практичної реалізації обрано базову бінарну модель (k = 2). Таке рішення обґрунтоване економічною та технічною доцільністю: бінарний алгоритм значно легший для інтеграції в наявну інфраструктуру, потребує генерації лише одного додаткового потоку із завадою й не вимагає дорогих транскодерів та кратного розширення CDN. Швидкодія близько 80 секунд для 1 млн глядачів є більш ніж достатньою, щоб заблокувати джерело ще до завершення першого раунду спортивної події.

4.6. Покроковий приклад роботи алгоритму

Розглянемо умовний приклад: трансляція з аудиторією N = 1 200 000 і одне джерело витоку. На першому кроці аудиторія ділиться навпіл: 600 000 отримують сегмент із завадою, решта 600 000 — чистий. Екстрактор фіксує заваду на піратському стрімі — отже, джерело у першій половині, а друга відкидається. Далі ці 600 000 знову діляться навпіл, і так далі. Динаміку показано в таблиці 4.3: за 21 ітерацію (84 с при сегменті 4 с) коло звужується від мільйона до одного облікового запису.

Таблиця 4.3 — Динаміка звуження множини підозрюваних (N = 1 200 000)

Ітерація	Підозрюваних залишилося	Дія системи
0	1 200 000	Виявлено факт витоку, запуск пошуку
1	600 000	Поділ навпіл, завада → реакція стріму
5	37 500	Звуження кола у 32 рази
10	1 172	Звуження кола у 1024 рази
15	37	Локалізовано малу групу
20	2	Залишилося два кандидати
21	1	Єдиний підозрюваний — перехід до верифікації

Висновки до розділу 4

Формалізовано метод активного трасування на основі динамічної дихотомії. Використання контрольної завади як зондувального сигналу у замкненому циклі дає логарифмічну швидкодію $O(\log_2 N)$ і дозволяє приймати рішення за фактом появи завади на стрімі, без накопиченого коду. Порівняння стратегій пошуку обґрунтувало дихотомію, а аналіз масштабування — бінарну модель ($k = 2$) як економічно та технічно доцільну.

РОЗДІЛ 5 АРХІТЕКТУРА МОДУЛІВ ТА ТЕХНІЧНА РЕАЛІЗАЦІЯ

У цьому розділі описано, як метод реалізується технічно. Йдеться про загальну будову системи, природу самої контрольної завади, принципи її непомітного вбудовування, роботу модуля розпізнавання, стійкість маркера до різних перетворень, процедуру фінальної верифікації та інтеграцію з наявними сервісами провайдера. Мета — показати, що метод не є тільки теоретичним: він реалізується звичайними засобами цифрової обробки сигналів і комп'ютерного зору.

5.1. Загальна архітектура: площина керування та площина даних

Запропоновану систему доцільно структурувати за принципом розділення на площину даних (Data Plane) та площину керування (Control Plane), що є типовим для масштабованих мережевих систем. Площина даних відповідає за безпосередню доставку медіаконтенту глядачам і включає стандартні компоненти пайплайну: кодувальник, пакувальник, точку походження та CDN. Площина керування містить інтелектуальні модулі захисту, що приймають рішення та керують поведінкою площини даних, не втручаючись у саму доставку для більшості користувачів.

Ключовими компонентами площини керування є: модуль вбудовування контрольної завади, що заздалегідь готує марковані варіанти сегментів; маніпулятор плейлистів, що адресно підмінює сегменти у маніфестах для обраних груп; модуль моніторингу та екстракції, що аналізує перехоплені піратські стріми; центральний модуль ідентифікації, що реалізує логіку дихотомічного пошуку та керує ітераціями; модуль фінальної верифікації; інтерфейс взаємодії із сервером DRM для відкликання ліцензій.

Така архітектура забезпечує мінімальний вплив на основний потік доставки: для звичайного глядача система працює абсолютно прозоро, а активність площини керування зосереджується лише навколо тих груп, у яких триває пошук джерела витоку. Це гарантує, що впровадження захисту не погіршує QoE для законослухняної аудиторії.

Рисунок 5.1 — Оригінальний кадр відеопотоку прямої трансляції без вбудованої контрольної завади

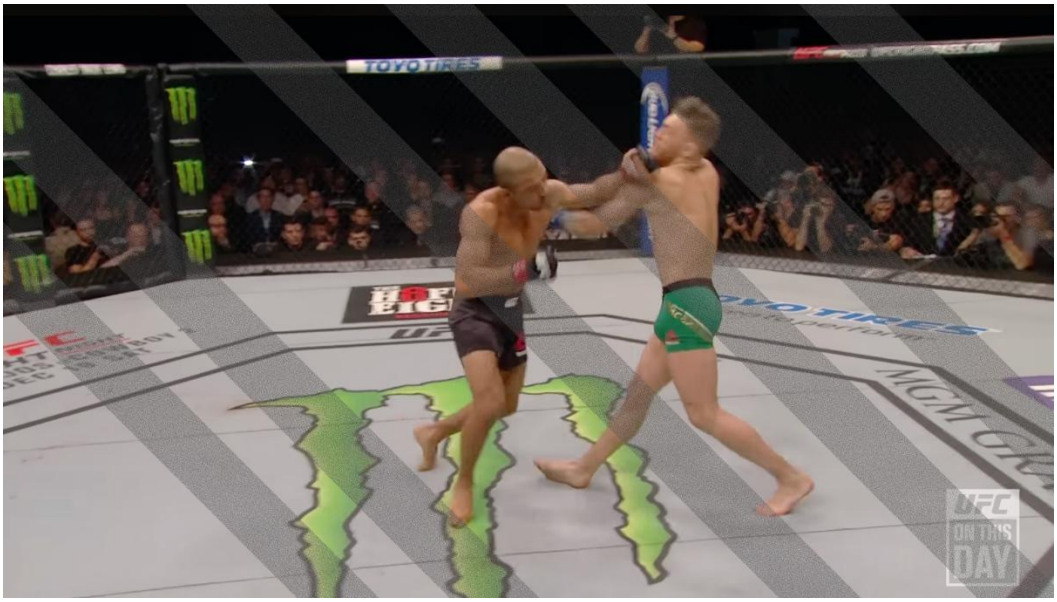

Рисунок 5.2 — Кадр того ж відеопотоку з вбудованою контрольною завадою. Амплітуду маркера на ілюстрації штучно збільшено для наочності; у робочому режимі система використовує значно слабший сигнал, непомітний для людського ока, але достатньо стійкий для зчитування екстрактором.

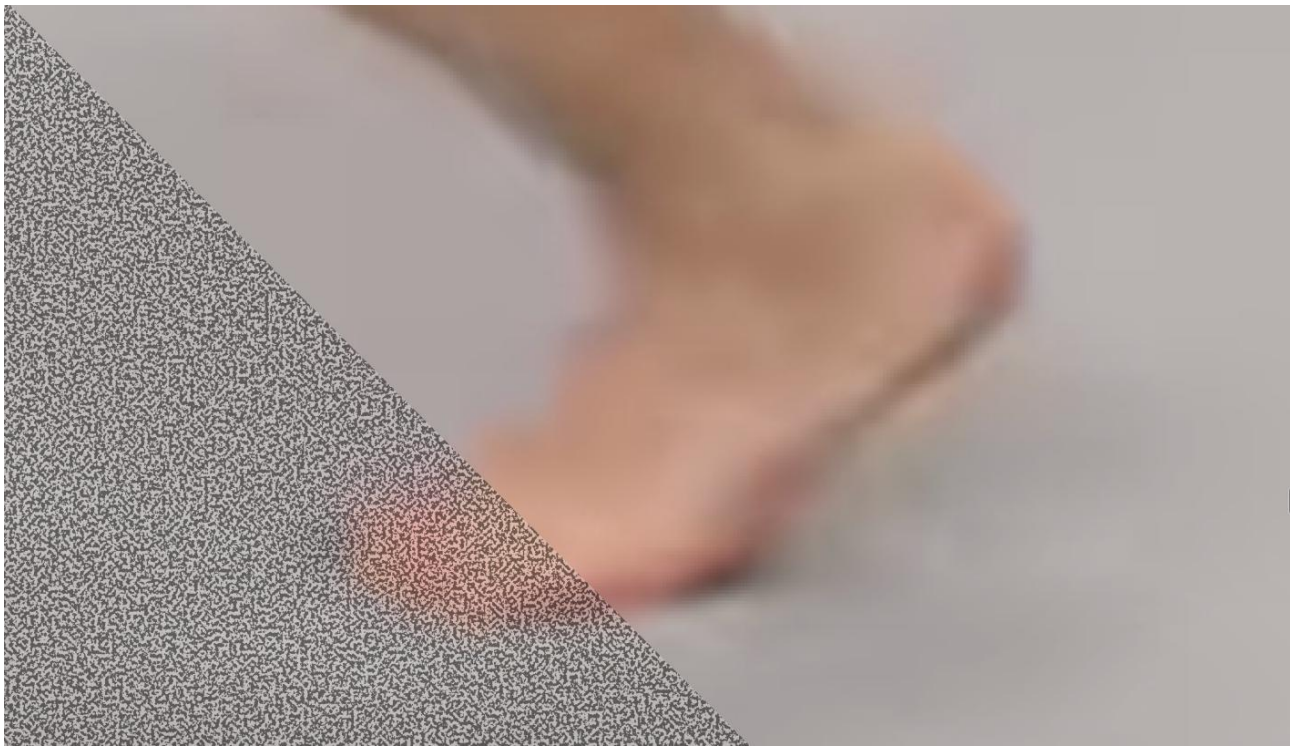

Рисунок 5.3 — Збільшений фрагмент кадру з вбудованою контрольною завадою: видно псевдовипадкову шумоподібну структуру маркера у каналі яскравості, що імітує природний шум сенсора камери

5.2. Фізична природа «контрольної завади» та просторове маскування

Контрольна завада фізично — це стеганографічний маркер, що вбудовується у відеопотік на етапі підготовки еталонних сегментів. Завада не є рівномірним зміщенням яскравості (легко детектується корекцією експозиції), а базується на псевдовипадковій шумоподібній текстурі малої амплітуди, що імітує природний шум сенсора камери й не привертає уваги.

Зміни вносяться переважно у канал яскравості (Y) колірної моделі YUV. Уточнімо поширене хибне твердження: людський зір **чутливіший саме до яскравості, ніж до кольоровості** (саме тому в кодуванні застосовують субдискретизацію хроми 4:2:0). Непомітність маркера досягається не вибором каналу, а використанням ефекту **просторового маскування яскравості (luminance masking)** [3]: високочастотний шум малої амплітуди вбудовується у текстурно насичені ділянки кадру (трава поля, натовп, складні фактури), де чутливість зорової системи до локальних коливань знижена. Адаптивне

регулювання амплітуди (perceptual shaping) — у гладких ділянках знижується, у текстурованих підвищується — оптимально розв'язує компроміс між непомітністю та стійкістю.

Геометрична організація шаблону

Для стійкості до перекодування шум обмежується чіткими геометричними шаблонами (Spatial Masking) — кількома паралельними діагональними смугами. Це зумовлено: 1) ортогональністю до структури кадру (об'єкти та межі блоків DCT мають горизонтальну/вертикальну орієнтацію, діагональ 45°/135° є чужорідною, що дозволяє відокремити її фільтрами); 2) стійкістю до геометричних перетворень (кут нахилу зберігається при масштабуванні та зміні сторін); 3) стабільністю при низькому бітрейті (форма смуг переживає квантування, аналізується енергетика шаблону, а не окремі пікселі).

5.3. Варіативність геометричних шаблонів для k-арного пошуку

При масштабуванні до k-арного дерева аудиторія на кожній ітерації ділиться на k груп, що вимагає генерації k еталонних потоків: одного чистого та $k-1$ потоків із різними завадами. Принципово важливо, що формування варіантів завади має базуватися на зміні просторової конфігурації шаблону, а не на зміні інтенсивності шуму.

Спроба кодувати варіанти градаціями інтенсивності (наприклад, 5 %, 10 %, 15 %) є хибною: алгоритми компресії H.264/H.265 усереднюють мікроскопічні коливання яскравості у блоках, унаслідок чого різні рівні інтенсивності зливаються й стають нерозрізненними на етапі екстракції після перекодування. Натомість геометричні (структурні) відмінності зберігаються значно надійніше. Тому масштабування реалізується виключно через зміну геометрії шаблонів. Наприклад, для $k = 4$ конфігурація така:

1. Група 1 — еталонний сегмент (відсутність завади).
2. Група 2 — діагональні смуги під кутом 45°.
3. Група 3 — діагональні смуги під кутом 135°.
4. Група 4 — горизонтальні смуги (0°).

При подальшому збільшенні k застосовуються додаткові конфігурації: вертикальні смуги (90°), перехресні (сітчасті) структури, пунктирні шаблони, зміна просторової частоти смуг (їх щільності). Модуль екстракції фіксує не амплітуду сигналу, а його структурні властивості — домінуючий кут нахилу та форму шаблону, які є інваріантними до перекодування та зміни масштабу. Така кодова система фактично перетворює простір геометричних орієнтацій на алфавіт символів для трасування.

5.4. Модуль розпізнавання (екстрактор)

Екстрактор функціонує на стороні сервера безпеки (у площині керування) і безперервно моніторить перехоплений нелегальний потік, виявляючи маркер та визначаючи його конфігурацію в реальному часі. Робота — у три кроки. Перший: покадрове захоплення та частотна фільтрація. Корисне зображення формується низькочастотними складовими, завада — високочастотним шумом; просторові високочастотні фільтри (оператор Лапласа, смугові фільтри) пригнічують фон, залишаючи різкі перепади яскравості маркера. Другий: аналіз геометричної структури. На відфільтрованому кадрі застосовується перетворення Хафа [16] (виявлення прямих ліній та їхнього нахилу навіть за наявності шуму) і двовимірний амплітудний спектр Фур'є (періодичні смуги дають характерні піки) — визначається домінуючий вектор спрямованості. Третій: компенсація геометричних маніпуляцій. Кут нахилу інваріантний до масштабування; при обрізанні країв всередині видимої ділянки зберігаються паралельність та орієнтація. Аналізується цілісна енергетика шаблону, не окремі пікселі — це дає стійкість до часткової втрати даних при низькому бітрейті.

Результат — бінарний (для k = 2) або k-арний звіт: відсутність шуму («чистий потік») або ідентифікація конкретного шаблону (наприклад, «нахил 45°»). Цей параметр передається до центрального модуля ідентифікації як вхідна змінна для наступної ітерації дихотомічного пошуку.

5.5. Стійкість маркера до перетворень

Придатність маркера для практики залежить від того, чи витримує він перетворення, що виникають при ретрансляції. Розглянемо найважливіші з них.

- **Перекодування.** Майже завжди застосовується піратом. Стійкість дає розміщення маркера у каналі яскравості та енергетично концентровані геометричні структури.
- **Масштабування, зміна сторін.** Кутова орієнтація смуг не залежить від розміру кадру.
- **Обрізання, накладання інтерфейсу.** Шаблон реконструюється за будь-яким видимим фрагментом.
- **Фільтрація.** Сильне розмиття знищує і якість самого піратського відео — компроміс завжди залишає маркер хоча б частково детектованим.

Найскладніша атака — змова: кооперація кількох порушників може заплутати бінарний сигнал. Базова модель її не закриває; це предмет надбудови стійкими до коаліцій кодами і напрям подальших досліджень.

5.6. Фінальна верифікація та ініціація блокування

Будь-яка автоматизована система протидії піратству повинна функціонувати з мінімальним рівнем хибних спрацьовувань, оскільки неправомірне блокування легального користувача є неприпустимим як з етичних, так і з репутаційних та юридичних міркувань. Тому алгоритм містить обов'язковий етап фінальної верифікації, що ініціюється, коли дихотомічний пошук звужує множину підозрюваних до одного унікального ідентифікатора (User ID).

Для остаточного підтвердження маніпулятор плейлистів одноразово інтегрує у потік підозрюваного спеціальний «Сегмент С» з візуально помітним, але короткочасним маркером — напівпрозорим QR-кодом із зашифрованими даними сесії або буквено-цифровим ідентифікатором, накладеним поверх відеоряду. Маркер відображається протягом короткого проміжку (0,5–1 с),

достатнього для надійної фіксації системою моніторингу. Оскільки цей сегмент надсилається виключно одному вже локалізованому підозрюваному, його поява на конкретному піратському стрімі є однозначним доказом джерела витоку.

Після успішного зчитування верифікаційного маркера центральний модуль безпеки генерує команду до сервера DRM з вимогою негайного відкликання авторизаційного токена та анулювання ліцензії на дешифрування для скомпрометованого облікового запису. Це призводить до миттєвого припинення видачі ключів, неможливості дешифрування подальших сегментів та повного обриву піратської трансляції біля її джерела — незалежно від того, на якій сторонній платформі вона велася.

5.7. Інтеграція з інфраструктурою провайдера

Перевага методу — у тому, що його можна вмонтувати в наявну інфраструктуру OTT-провайдера без її докорінної перебудови. Модуль вбудовування завади працює поряд із наявним шифруванням на етапі пакування; маніпулятор плейлистів реалізується як проміжний шар перед видачею маніфестів (це вже типово для систем персоналізованої реклами) [20, 21]; взаємодія з DRM іде через стандартні інтерфейси відкликання ліцензій. Повний цикл роботи: виявлення факту витоку → дихотомічний пошук (на кожній ітерації — формування груп, підміна сегментів, аналіз реакції) → локалізація єдиного кандидата → фінальна верифікація Сегментом С → команда DRM на відкликання ліцензії. Як показано далі у розділі 6, цикл укладається у десятки секунд.

5.8. Контроль хибних спрацьовувань

Промислова система не має права помилково блокувати чесного користувача. Основний запобіжник — обов'язкова фінальна верифікація видимим маркером (Сегмент С) перед блокуванням: ніяке рішення не приймається лише за результатами проміжних ітерацій. Додатково на кожній ітерації результат екстрактора підтверджується на кількох послідовних кадрах, що згладжує одиничні шуми. Відмовостійкість забезпечується резервуванням

модулів моніторингу та екстракції, а ведення журналу аудиту (audit trail) з часовими мітками та підписами формує юридично придатну доказову базу.

Висновки до розділу 5

Побудовано технічну архітектуру системи з поділом на площини даних і керування. Контрольна завада — високочастотний шумоподібний сигнал у каналі яскравості, організований у геометричні шаблони; її непомітність і стійкість до перекодування забезпечує перцептивне маскування у текстурованих ділянках кадру. Екстрактор працює у три кроки — фільтрація, аналіз геометрії через перетворення Хафа, компенсація геометричних маніпуляцій. Завершальна верифікація видимим маркером виключає хибні спрацьовування, а взаємодія з DRM блокує джерело незалежно від платформи ретрансляції.

РОЗДІЛ 6 ОЦІНКА ЕФЕКТИВНОСТІ ЗАПРОПОНОВАНОГО РІШЕННЯ НА ПРИКЛАДІ РЕАЛЬНОЇ ТРАНСЛЯЦІЇ

6.1. Аналіз вхідних даних та масштабів піратства

Щоб оцінити роботу методу в реальних умовах, застосуємо його модель до конкретної комерційної події з високими навантаженнями та значним рівнем нелегальної ретрансляції. За приклад взято поєдинок за звання абсолютного чемпіона світу у надважкій вазі між Олександром Усиком і Тайсоном Ф'юрі — фінальний бій серії, що відбувся 21 грудня 2024 р. в Ер-Ріяді. Подія транслювалася за моделлю Pay-Per-View, тобто є найбільш привабливою мішенню для піратів.

За даними бродкастерів, поєдинки серії згенерували понад 1,5 млн платних PPV-підключень — беремо це число як базу одночасно активних легальних глядачів у мережі CDN: N = 1 500 000. Аналіз Yield Sec (за матеріалами Mail Sport) показав, що подію нелегально подивилися щонайменше 20 мільйонів осіб [22]; втрати DAZN, Sky Sports і TNT Sports перевищили 100 млн доларів. Географічно піратський трафік розподілявся так: 45 % — Європа, 25 % — Північна Америка, 16 % — Азія.

Важливо чітко розділити: нелегальний глядач — це одне, а джерело витоку (пірат, що перетранслює) — зовсім інше. Запропонований метод націлений саме на другу категорію — на легальні акаунти, які знімають екран і пускають це далі. За тим самим звітом, зафіксовано близько 2 000 окремих піратських трансляцій [22, 23]. Беремо P = 2 000. Середня аудиторія на один піратський стрім:

$$20\ 000\ 000 / 2\ 000 = 10\ 000 \text{ глядачів на один стрім}$$

Відносний масштаб загрози:

Частка джерел витоку відносно легальної аудиторії, що відображає складність задачі пошуку:

$$R = P / N = 2\ 000 / 1\ 500\ 000 \approx 0{,}00133 \approx 0{,}133\ \%$$

Отже, порушники становлять лише близько 0,133 % легальної аудиторії. Це класична проблема «голки в копиці сіна»: традиційні системи пасивного моніторингу витрачають години на виявлення цих часток відсотка серед півтора мільйона користувачів, тоді як комерційна цінність трансляції (що триває близько години) за цей час вичерпується.

6.2. Моделювання часу та ітерацій для ізоляції множинних порушників

Задача: знайти множину з P = 2 000 порушників серед N = 1 500 000 підключень. Послідовний пошук кожного окремо мав би складність $O(P \cdot \log_2 N)$, що неприйнятно довго. Тому застосовуємо паралельну ізоляцію. Для одного пірата діє класичне адаптивне звуження — половина без порушника відкидається, потрібно $\lceil \log_2 N \rceil$ кроків. Коли порушники розосереджені по обох групах, відкидати половину не можна: алгоритм узагальнюється, обидві гілки дерева одночасно поділяються навпіл, а екстрактор моніторить усі піратські стріми паралельно. Поява чи відсутність завади на кожному окремому стрімі визначає, у яку підгрупу він потрапляє.

Ключове: всі піратські стріми спостерігаються одночасно, кожна ітерація поглиблює усі гілки на один рівень — тож максимальна кількість кроків залежить лише від глибини дерева для початкової множини N і не залежить від кількості порушників P. Розрахунок:

$$I = \lceil \log_2 N \rceil = \lceil \log_2 1\,500\,000 \rceil = 21 \text{ ітерація}$$

При тривалості сегмента T_сег = 4 с:

$$T\_дет = I \cdot T\_сег = 21 \cdot 4 = 84 \text{ секунди}$$

Оскільки один раунд триває 3 хвилини, система локалізує та заблокує всі 2 000 джерел ще до екватора першого раунду. Зауваження: 84 с — нижня (теоретична) оцінка. Реально до неї додається затримка піратського каналу (буферизація, перекодування), що для Twitch або Telegram може становити десятки секунд. Тому коректніше: метод не усуває витік миттєво, а радикально скорочує вікно його існування.

6.3. Математична та логічна оцінка ефективності блокування (K_1 проти K_2)

Основа розрахунку — загальна кількість активних піратських ретрансляцій, виявлених моніторингом: K_в (цільова база для нейтралізації, 100 % виявлених загроз).

Традиційна модель делегує блокування кінцевим платформам, на яких відбувається ретрансляція:

$$K_1 = K\_авто + K\_ручн$$

де K_авто — трансляції, заблоковані внутрішніми алгоритмами платформи (Content ID); K_ручн — заблоковані за запитом правовласника (DMCA Takedown) під час ефіру. Проте традиційна модель безсила проти трансляцій у закритих або незалежних екосистемах:

$$K\_в = K_1 + K\_неблок$$

де K_неблок — виявлені, але незаблоковані трансляції: закриті групи месенджерів (Telegram), тіньові IPTV, автономні піратські сайти, скарги з часом розгляду більше за тривалість події. Коефіцієнт ефективності традиційної системи:

$$E_1 = K_1 / K\_в$$

Запропонована архітектура впливає не на платформу-розповсюджувача, а на джерело сигналу — легальний плеєр порушника. Оскільки система інтегрована у внутрішню інфраструктуру провайдера, для неї не має значення, куди саме пірат передає потік. Якщо екстрактор фіксує заваду на будь-якому виявленому стрімі з множини K_в, алгоритм гарантовано ізолює та відключить джерело через відкликання ліцензії дешифрування:

$$K_2 = K\_в - K\_похиб$$

де K_похиб — незаблоковані через системні збої (у штатному режимі прямує до нуля). Відповідно:

$$E_2 = K_2 / K\_в \approx 1$$

Уточнення: величина K_в обмежена можливостями моніторингу — щоб зчитати заваду, треба спершу отримати доступ до стріму. Це спільна вимога для обох моделей. Принципова перевага запропонованого методу — на етапі нейтралізації: для будь-якої виявленої трансляції з K_в система блокує джерело на рівні DRM незалежно від співпраці платформи.

Приймемо K_в = 2 000. За галузевою практикою, значна частка трансляцій розміщується на платформах, що не реагують на запити під час Live-ефіру. Припустимо (як модельне допущення), що лише близько 40 % вдається заблокувати традиційною моделлю в межах ефіру: $K_1 \approx 800$, K_неблок ≈ 1 200. Для запропонованого методу K_похиб ≈ 0, тому $K_2 \approx 2\ 000$. Результати — у таблиці 6.1.

Таблиця 6.1 — Порівняння ефективності блокування під час прямого ефіру

Показник	**Традиційна модель (K_1)**	**Запропонований метод (K_2)**	**Од.**
Виявлено трансляцій (K_в)	2 000	2 000	шт.
Заблоковано під час ефіру	≈ 800	≈ 2 000	шт.
Не нейтралізовано	≈ 1 200	≈ 0	шт.
Коефіцієнт ефективності (E)	≈ 0,40	≈ 1,00	—
Частка нейтралізації	40 %	≈ 100 %	—

Математичне співставлення двох моделей базується на наявності неконтрольованої множини K_неблок у першому випадку та її практичній відсутності у другому. Звідси випливає строга нерівність:

$$E_1 = K_1 / K\_в \ < \ E_2 = K_2 / K\_в$$

$$0{,}40 \ < \ 1{,}00$$

6.4. Аналіз чутливості

Перевіримо, наскільки висновок залежить від вибору параметрів. Розглянуто три фактори:

– **Розмір аудиторії N.** Через логарифмічну залежність $I = \lceil \log_2 N \rceil$ зростання N удесятеро (з 1,5 млн до 15 млн) додає лише 3–4 ітерації — час трасування з 84 до 96 с. Метод відмінно масштабується.
– **Тривалість сегмента T_сег.** При HLS 6 с маємо 126 с; при LL-HLS 1–2 с — 21–42 с. Поширення низьколатентних протоколів додатково покращує результат.
– **Частка блокування у традиційній моделі.** Навіть оптимістичні 60 % ($E_1 \approx 0{,}60$) усе одно поступаються $E_2 \approx 1{,}00$. Перевага зумовлена структурно — наявністю непідконтрольної множини K_неблок, а не конкретними числами.

6.5. Обмеження запропонованого методу

Чесне окреслення меж застосовності методу необхідне для коректної інтерпретації отриманих результатів і визначення напрямів подальшого розвитку.

– **Чутливість до змови.** Базова бінарна модель розрахована на одиничне некооперативне джерело; кооперація кількох порушників потребує надбудови стійкими до коаліцій кодами (Тардоса, Боне–Шоу).
– **Залежність від моніторингу.** Величина K_в обмежена здатністю системи виявити та отримати доступ до піратського стріму; джерела, недоступні для моніторингу, залишаються поза дією методу.
– **Реальна затримка.** Фактичний час трасування перевищує теоретичні 84 с на величину затримки піратського каналу, тому метод скорочує вікно витоку, а не усуває його миттєво.

Висновки до розділу 6

Розрахунки на даних реальної події підтвердили практичну спроможність методу. За аудиторії $N = 1\,500\,000$ і тривалості сегмента 4 секунди весь масив із приблизно 2 000 піратських джерел ізолюється за 21 ітерацію — це близько 84 секунд ефірного часу, тобто ще до екватора першого раунду. Виведена нерівність $K_1/K\_в < K_2/K\_в$ і чисельний результат $E_1 \approx 0{,}40$ проти $E_2 \approx 1{,}00$ показують, що нейтралізація на рівні інфраструктури провайдера працює фундаментально краще, ніж залежність від реакції сторонніх платформ. Аналіз

чутливості переконує, що такий висновок не залежить від випадкового вибору параметрів. У сумі швидкодія та повнота блокування роблять незаконну ретрансляцію економічно безглуздою.

ЗАГАЛЬНІ ВИСНОВКИ

У роботі розв'язано актуальне завдання підвищення захищеності цифрового медіаконтенту комерційних прямих трансляцій в умовах вразливостей кінцевого відтворення відеоданих. За результатами дослідження зроблено такі висновки:

1. Проаналізовано процес і проблемні питання комерційних прямих трансляцій. Установлено, що ключовими загрозами є «аналогова діра», негативний вплив захисту на затримку та QoE, проблема «шквального натовпу» й найбільш руйнівна — незаконна редистрибуція за моделлю «один-до-багатьох», проти якої традиційні засоби безсилі, оскільки пірат є технічно легальним клієнтом.
2. Проаналізовано наявні рішення щодо захисту контенту прямих трансляцій (контроль доступу, шифрування AES, DRM, традиційні водяні знаки) та виявлено їх обмеження: жоден із них не забезпечує швидкої ідентифікації зловмисника за низького навантаження на кінцевий пристрій.
3. Модифіковано систему захисту шляхом застосування методу активного ітеративного трасування на основі динамічної дихотомії. На відміну від пасивного маркування, метод використовує контрольну заваду як зондувальний сигнал у замкненому циклі зворотного зв'язку та ідентифікує джерело за фактом появи завади на нелегальній ретрансляції, а не за накопиченою комбінацією сегментів. Обґрунтовано вибір бінарної моделі ($k = 2$) як економічно й технічно доцільної.
4. Оцінено ефективність запропонованого рішення за рахунок натурно-математичного моделювання на прикладі реальної трансляції (Усик — Ф'юрі). Показано, що за $N = 1\,500\,000$ і $T_{сег} = 4$ с метод ізолює всі $\approx 2\,000$ джерел витоку за 21 ітерацію (≈ 84 с), тобто ще до середини першого раунду. Коефіцієнт ефективності (K — доля заблокованих протиправних трансляцій серед виявлених протиправних трансляцій) зріс з 0,40 до 1,00.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Arnold M., Schmucker M., Wolthusen S. D. Techniques and Applications of Digital Watermarking and Content Protection. Norwood : Artech House, 2003. 274 p.
2. Cheng H. C., Jiang H. V., Wang C. J. A New Dynamic Traitor Tracing Scheme for Broadcast Encryption. IEEE Transactions on Information Forensics and Security. 2007. Vol. 2, No. 3. P. 548–558.
3. Cox I. J., Miller M. L., Bloom J. A. et al. Digital Watermarking and Steganography. 2nd ed. Burlington : Morgan Kaufmann, 2007. 624 p.
4. Doërr G., Dugelay J. L. A Guide Tour of Video Watermarking. Signal Processing: Image Communication. 2003. Vol. 18, No. 4. P. 263–282.
5. Fiat A., Tassa T. Dynamic Traitor Tracing. Journal of Cryptology. 2001. Vol. 14, No. 3. P. 211–223.
6. Boneh D., Shaw J. Collusion-Secure Fingerprinting for Digital Data. IEEE Transactions on Information Theory. 1998. Vol. 44, No. 5. P. 1897–1905.
7. Tardos G. Optimal Probabilistic Fingerprint Codes. Journal of the ACM. 2008. Vol. 55, No. 2. P. 1–24.
8. ISO/IEC 23001-7:2016. Information technology — MPEG systems technologies — Part 7: Common encryption in ISO base media file format files. Geneva : ISO, 2016.
9. ISO/IEC 23009-1:2022. Information technology — Dynamic adaptive streaming over HTTP (DASH) — Part 1: Media presentation description and segment formats. Geneva : ISO, 2022.
10. Pantos R., May W. HTTP Live Streaming. RFC 8216. Internet Engineering Task Force (IETF), 2017. 60 p.
11. ITU-T Recommendation H.264. Advanced video coding for generic audiovisual services. Geneva : ITU, 2021.
12. ITU-T Recommendation H.265. High efficiency video coding (HEVC). Geneva : ITU, 2021.
13. Encrypted Media Extensions. W3C Recommendation. World Wide Web Consortium (W3C), 2017. URL: https://www.w3.org/TR/encrypted-media/.

14. National Institute of Standards and Technology (NIST). FIPS PUB 197: Advanced Encryption Standard (AES). Gaithersburg : NIST, 2001.
15. Stallings W. Cryptography and Network Security: Principles and Practice. 7th ed. London : Pearson, 2017. 768 p.
16. Duda R. O., Hart P. E. Use of the Hough Transformation to Detect Lines and Curves in Pictures. Communications of the ACM. 1972. Vol. 15, No. 1. P. 11–15.
17. Nishimura R. et al. Watermarking Technologies for Broadcast Monitoring. Proceedings of the IEEE. 2012.
18. Seufert M., Egger S., Slanina M. et al. A Survey on Quality of Experience of HTTP Adaptive Streaming. IEEE Communications Surveys & Tutorials. 2015. Vol. 17, No. 1. P. 469–492.
19. Ma Z. et al. Mobile Video Delivery with HTTP. IEEE Communications Magazine. 2012.
20. Luntovskyy A., Gubarev D. Modern Video Streaming Technologies. Cham : Springer, 2022.
21. Unified Streaming. Forensic Watermarking with Unified Packager: Server-side watermarking architecture. Technical Whitepaper. Amsterdam, 2020.
22. Yield Sec / Mail Sport. Analysis of illegal streaming of the Usyk vs. Fury heavyweight bout. 2024. URL: https://www.dailymail.co.uk/sport/boxing/.
23. MUSO. Global Piracy & Streaming Trends Report: Live Sports Piracy. London : MUSO, 2024.
24. Synamedia. The State of Sports Piracy: Tackling Illegal Streaming. Technical Report. 2024.л
25. Миронюк І.А.; Курдеча В.В. // Модифікована система захисту контенту комерційних прямих трансляцій // Перспективи розвитку інформаційно-телекомунікаційних технологій та систем (ПРІТС-2026) : тези XVIII наук.-техн. Конф. Студентів та аспірантів, 13–17 квіт. 2026 р., Київ. – Київ : КПІ ім. Ігоря Сікорського, 2026. – С. 424.