торой выделяются идентификационные признаки – регулярные спектральные компоненты.

Отметим, что других методов и средств, позволяющих идентифицировать АЦЗАС, по нашим сведениям, не существует.

Добавим, что в программе заложены дополнительные функции, обеспечивающие удобство работы эксперта, например представление во временной и спектральной областях исследуемой сигнаграммы в разных окнах с их взаимной синхронизацией.

Разработан и банк данных, заполняемый в процессе проведения экспертиз и позволяющий использовать эти данные совместно с полученными результатами исследований для быстрого оформления экспертного заключения.

По нашему мнению, подобная методология разработки средств и методик экспертных исследований, основанная на системном анализе, может быть приложима к экспертизе любых технических объектов, позволяет обеспечить научную обоснованность и тщательную отработку средств и методик их проведения.

С. М. Бобрицький, завідувач лабораторії Харківського НДІСЕ,
С. В. Стороженко, молодший науковий співробітник Харківського НДІСЕ

ДОСЛІДЖЕННЯ ОЗНАК МОНТАЖУ ЗАПИСІВ, ВИКОНАНИХ ЦИФРОВИМИ ЗАПИСУЮЧИМИ ПРИСТРОЯМИ

Розглянуто сформовані на теперішній час напрямки досліджень ознак монтажу фонограм, виконаних цифровими записуючими пристроями, а також перспективи дослідження цифрових матеріалів і засобів звукозапису.

Рассмотрены сформированные в настоящее время направления исследований признаков монтажа фонограмм, выполненных цифровыми записывающими устройствами, а также перспективы исследований цифровых материалов и средств звукозаписи.

Одним з найважливіших діагностичних завдань фоноскопічної експертизи є дослідження ознак монтажу. Традиційними об'єктами дослідження до останнього часу були носії на магнітній стрічці, частка яких в досліджуваних матеріалах постійно зменшується завдяки виробникам звукозаписуючих пристроїв і новим телекомунікаційним технологіям фіксування та передачі мовлення й зображення. У цій статті ми не зупинятимемося на особливостях установлення ознак монтажу в записі звуку на них. Ці об'єкти дослідження мають значну історію їхнього використання та відповідно достатньо відомі методи дослідження. Цифрова апаратура запису (ЦАЗ) має відносно

невеликий строк використання, але за своєю «комунікативністю», відносною простотою, достатньою якістю зафіксованого мовленнєвого сигналу, доступною вартістю стала конкурентоспроможною альтернативою записуванню на магнітну плівку.

Під традиційним розумінням поняття «визначення ознак монтажу» мається на увазі таке тлумачення: дослідження звуко-, відеозаписів з метою встановлення наявності / відсутності ознак монтажу чи змін, унесених у процесі фіксування запису чи після нього. Стосовно цифрових записів ці змінення можуть мати як частковий, так і загальний характер. До часткових змінень належать:

— вирізання ділянок запису, подальше редагування програмними засобами при безпосередньому з'єднанні ЦАЗ із комп'ютерною технікою за допомогою спеціальних програмних і апаратних засобів та підміна оригіналу запису;

— дописування ділянок запису чи виконання вставок з інших записів, змінення місцями блоків даних (виконані за тією самою технологією).

До змінень, що мають загальний характер, належать:

— змінення технічних параметрів запису (формату потоку, дозволяючих властивостей потоку, частоти дискретизації, виду бітрейта, кількості потоків, протоколів стискання);

— змінення відображення середовища, притаманного обставинам запису.

У будь-якому разі часткові й загальні змінення включають перетворення, породжені комплексом дій, які і є ознаками монтажу, загальну характеристику котрого наведено в ГОСТ 13699-91, де під монтажем розуміється об'єднання двох або більше частин однієї чи декількох раніше записаних фонограм шляхом перезаписування, під час якого можуть вноситися змінення в записувану інформацію та може змінюватися черговість фрагментів.

Звуковий чи відеофайл цифрового запису як об'єкт криміналістичного дослідження сучасними програмно-апаратними засобами досліджується як з точки зору внутрішньої цифрової структури, так і у вигляді уявлення потоків мовленнєвого сигналу та фреймів відеоряду, де візуалізуються особливості розподілу мовленнєвого сигналу (фреймів відеоряду) в часі й загальному спектрі запису. У країнах СНД найбільшими досягненнями в цьому напрямку є відомі програмно-апаратні комплекси криміналістичного дослідження звукозаписів: ИКАР з програмними пакетами SIS, EditCleiner, SoundTracker (Санкт-Петербург); Justiphone та OT Expert (Москва); програма «Академія» (Київ). У зв'язку з тим, що ці комплекси мають достатньо високу ринкову вартість, а їхні відомі можливості в дослідженні внутрішньої структури файлів необхідно поглиблювати, експерти Харківського НДІСЕ в цьому році виконують науково-дослідницьку роботу, мета якої

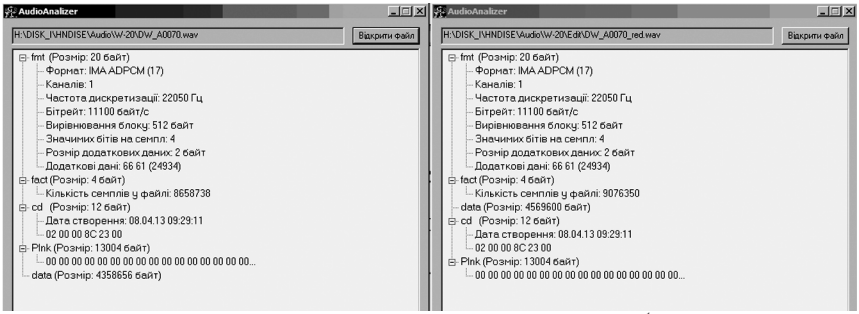
полягає у вивченні особливостей фіксування мовленнєвого сигналу у форматах запису, що найбільш часто використовуються в ЦАЗ (точніше в цифрових диктофонах), і виділенні притаманних цим форматам ознак.

Незважаючи на велику різноманітність цифрових записуючих пристроїв, форматів даних, які використовуються в них, досить небагато. Зазвичай це один з таких форматів файлів: wav, mp3, wma, amr. Для аналізу записаних файлів у Харківському НДІСЕ розробляється програмний пакет AudioAnalizer, призначений для аналізу інформації на рівні форматів файлів. Нижче надано скорочений опис результатів дослідження найбільш поширених форматів.

Формат WAV (або WAVE) розроблено для персональних комп'ютерів компаніями Microsoft та IBM, у якому жоден с аудіокодеків не резервується для використання, файли являють собою контейнер, у якому зберігається аудіопотік, закодований одним із різноманітних кодеків. Найчастіше застосовується кодек PCM. Маркер типу файлу розміщується з початку та має таку структуру: 4 символи RIFF, 4 байти розміру файлу, 4 символи WAVE. За маркером починаються блоки даних, які ще називаються чанками (від англ. chunk – кусень, частина чого-небудь). Кожен блок характеризується чотирьохсимвольним (максимальна кількість символів) ім'ям, яке визначає його тип. Стандартних блоків існує досить невелика кількість: fmt, fact, data, cue, plst, list, labl, ltxt, note, smpl, inst. Найважливішими є три блоки, які зберігають інформацію про кодек, що використовується (fmt), додаткову інформацію, яка залежить від кодека (fact), та сам потік даних (data). Інші типи блоків мають другорядне значення та майже не використовуються для експертного дослідження.

Як видно з розглянутого опису, файли цього формату мають дуже просту структуру, та не надають великої кількості можливостей для зберігання додаткової інформації або для її аналізу. Характерними ознаками як записуючих пристроїв, так і програм для редагування звукових файлів можуть бути тип кодека, що використовується, порядок розташування стандартних чанків, використання другорядних або нестандартних чанків.

Наприклад, під час записування файлу за допомогою диктофона Olympus W-20 додаються два нестандартні чанки: cd, який містить інформацію про дату створення файлу та має розмір 12 байт, і Plnk, який має розмір 13004 байти й заповнений нулями. Блоки записуються в такій послідовності: fmt, fact, cd, Plnk, data. У той самий час як після редагування цього файлу програмою Adobe Audition невідомі блоки розташовуються наприкінці файлу та послідовність має такий вигляд: fmt, fact, data, cd, Plnk. На рис. 1 зображено вікно програми AudioAnalizer з файлом, безпосередньо записаним за допомогою диктофона *(а)*, і після його редагування *(б)*.



а *б*

Рис. 1. Вікно даних файлу формату *.wav, записаного за допомогою цифрового диктофона Olympus W-20 (а) і відредагованого звуковим редактором Adobe Audition (б)

Майже єдиним засобом з'ясування призначення нестандартних блоків є збирання й аналіз блоків зі значної кількості файлів-зразків. Інформація про формат файлу та стандартні блоки є відкритою й легко знаходиться в мережі Інтернет.

Формат MP3 (MPEG-1 Audio Layer 3) – це потоковий формат кодування аудіоданих, названий так його розробниками Moving Picture Experts Group, створеної з експертів компаній Fraunhofer IIS та AT&T Bell Labs. Сам формат файлу не стандартизований і, як буде показано нижче, фактично в mp3 файлі можуть зберігатися будь-який з різних версій аудіопотоків: офіційні MPEG-1 і MPEG-2, неофіційний MPEG-2.5.

Файли цього формату фактично не мають форматної структури як такої, а є послідовністю mpeg фреймів у вигляді пар: заголовок і аудіодані. Нечисленні допоміжні структури теж зберігаються в межах фреймів. Офіційна інформація про структуру фреймів закрита, надається авторам програмного забезпечення та виробникам приладів за плату. Але й неофіційних даних достатньо, аби скласти досить повну картину.

Заголовок блоку даних (фрейму) має розмір 32 біти та містить такі бітові поля: маркер синхронізації; 11 біт, які мають значення одиницю; версія – MPEG; 1, 2, 2.5 – індекс пласта (layer) версії; I, II, III – прапор наявності контрольної суми (CRC16); бітрейт (від 8 до 448 кбіт/с) або ознака наявності змінного бітрейту (VBR); частота дискретизації (від 8 до 44 кГц); кількість каналів та декілька додаткових полів і прапорів.

Розмір даних, що зберігаються у фреймі, обчислюється з огляду на параметри, збережені в заголовку; він може бути постійним для усього файлу (для постійного бітрейту), так і змінюватися в разі застосування змінного бітрейту. Використання VBR, крім перерахунку розміру даних, також означає, що для встановлення

часу програвання потрібно проаналізувати заголовки всіх фреймів файлу. У цьому випадку в першому блоку даних файлу може зберігатись одна з таких структур: XING або VBRI заголовок.

Заголовок XING містить такі дані: маркер початку заголовку, 4 символи Xing або Info; прапори присутності параметрів (усі перелічені нижче параметри можуть бути відсутні в заголовку); кількість фреймів у файлі; кількість байтів у файлі; 100 індексів змісту файлу для швидкого пересування по ньому; показник якості кодування (0 – найкраще, 100 – найгірше).

Заголовок VBRI у свою чергу містить такі дані: маркер початку заголовку, 4 символи VBRI; номер версії; затримка; якість кодування; кількість байтів і фреймів у файлі; індекс змісту файлу для швидкого пересування по ньому.

Також програмні й апаратні засоби можуть додавати у файл власні дані. Напевне, найвідоміший приклад – це програмний кодек LAME, який додає власну службову інформацію як в перші, так і в останні фрейми файлу.

Крім власне аудіоданих, у файлі також може зберігатись інша інформація (зазвичай текстова) у вигляді тегів. Існує досить велика кількість форматів тегів, ми розглянемо тільки два найбільш поширених: ID3v1 та ID3v2. Не зважаючи на схожі назви, стандарти не мають ніякого відношення один до одного та були розроблені різними організаціями.

Теги формату ID3v1 зберігаються наприкінці файлу та мають досить примітивну структуру. Фактично це була перша спроба додати до mp3 метадані (опис змісту файлу). Якщо у файлі присутній тег ID3v1, останні 128 байтів містять такі дані: 3 символи маркера початку тегу TAG; 3 поля по 30 символів з назвами пісні та альбому, іменем виконавця; 4 символи року виходу альбому; 28 або 30 символів коментарю; 1 символ ознаки кінця коментарю. Якщо він нульовий, то коментар має довжину 28 символів, а далі йдуть два додаткових поля; 1 байт номера пісні в альбомі; 1 байт номера жанру (зі списку жанрів).

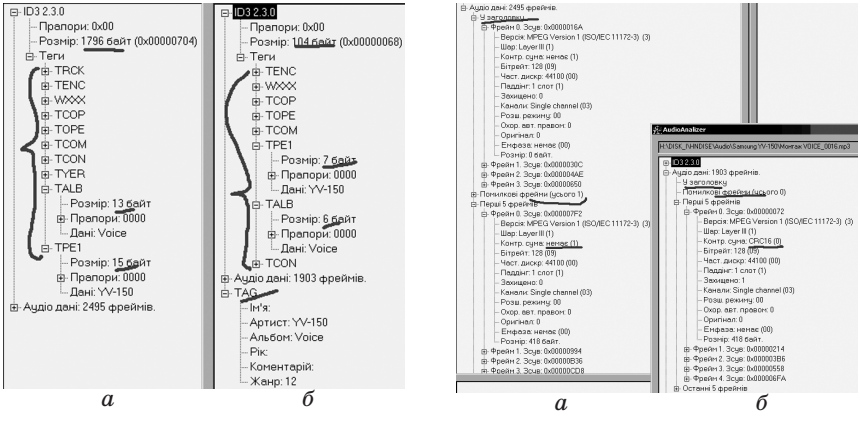
Крім основної, існує розширена версія тегу, вона зберігається у 227 байтах до початку основної та містить такі дані: 4 символи маркера початку тегу TAG+; 60 символів з назвами пісні та альбому, іменем виконавця (разом з попереднім TAG усього 90); 1 байт швидкості (0 – немає значення, 4 – найшвидше); 30 символів для жанру запису; 12 символів для часу початку та кінця відтворення у форматі mm:ss.

На відміну від свого попередника, теги формату ID3v2 зберігаються на початку файлів. Їхні структури відрізняються залежно від версії. Крім невеликих доповнень чи косметичних змінень, є й досить значні відмінності. Наприклад, ідентифікатори тегів, починаючи з версії 2.3.0, стали кодуватися чотирма символами замість

трьох. Нижче в спрощеному вигляді описано найновішу з існуючих версій – ID3v2.4.0. Заголовок: маркер наявності тегу «ID3»; 2 байти номеру версії; 1 байт прапорів; 4 байти розміру тегу (точніше, 4 по 7 біт, старший біт кожного байту не використовується). Слідом за ним може йти розширений заголовок, якій містить набір додаткових прапорів. Наявність розширеного заголовку визначається прапорами в основному. Для прискореного пошуку тегу при обробленні файлу з кінця тег може завершуватися копією заголовку з ідентифікатором «3DI». Інформація в тегу зберігається за допомогою фреймів. Вони мають таку структуру: 4 символи ідентифікатора фрейму; 4 байти (4 по 7 біт) розміру фрейму; 2 байти прапорів; інформація, що зберігається для даного типу фрейму. Це можуть бути як назви пісні та альбому, ім'я виконавця (фрейми TIT2, TPE1, TALB), так і текст пісні, або навіть зображення диска чи його обкладинки.

Характерними ознаками для цього типу файлів, крім характеристик аудіопотоку, можуть бути розширені mpeg-заголовки, додавання фреймів з нестандартною інформацією, версії тегів, що використовуються, інформація в тегах і послідовність фреймів. Також розробники як програмного, так і апаратного забезпечення зазвичай досить вільно підходять до дотримання стандартів ID3, що дозволяє експерту спиратися на розбіжності в реалізаціях.

Як бачимо на рис. 2, в оригінальному *(а)* та відредагованому *(б)* файлах присутні, крім змінення довжини потоку даних, такі розбіжності: різні розмірі тегів ID3v2; присутність тегу ID3v1; різна кількість фреймів у тегах; різна послідовність фреймів TCON, TALB, TPE1; різний розмір для фреймів с текстовими даними; наявність контрольної суми в аудіофреймах, помилкових фреймів і аудіофреймів (або даних, схожих на них) у місці, відведеному під ID3v2 тег.



а *б* *а* *б*

Рис. 2. Вікно даних файлу формату *.mp3, оригінального (*а*) і відредагованого звуковим редактором Adobe Audition (*б*)

Формат WMA (Windows Media Audio). Формат є псевдонімом для файлів формату ASF, розробленого фірмою Microsoft, у якому зберігаються тільки аудіодані (для файлів, які містять відеозаписи, зарезервовано інше розширення – WMV). Специфікація щодо цього формату доступна на сайті Microsoft, розповсюджується та може використовуватися безкоштовно, але ліцензія забороняє авторам відкривати вихідний код розроблених програмних засобів. Файли формату WMA являють собою контейнер метаданих. Формати збережених даних не регулюються специфікацію, для кодування аудіо/відеоінформації може використовуватися будь-який з доступних кодеків.

Дані у файлі зберігаються в спеціалізованих блоках, кожен з яких характеризується як найменше двома полями: унікальним ідентифікатором (GUID) і розміром. Верхній рівень структури файлу складається з таких блоків: заголовок, який містить інформацію про файл, потоки та ін.; блок з пакетами власне даних; індекс для прискореної навігації по файлу; блоки зі спрощеним індексом, інформацією про носій і з тайм кодами. З блоків верхнього рівня тільки заголовок містить інші блоки. Найважливіші з них (усього 16): інформація про файл; інформація про потоки; розширений заголовок; список кодеків; дані для корекції помилок; опис змісту файлу та його розширення.

Заголовок коректного файлу обов'язково має містити інформацію про файл, розширений заголовок і хоча б один блок стосовно потоку. Розширений заголовок містить додаткові блоки (усього 13), серед яких: додаткові параметри потоків, пріоритети потоків, список мов, розподіл каналів зв'язку тощо. Файл може містити тільки по одному блоку з характеристиками файлу та розширеним заголовком і один блок потоку на кожен потік даних.

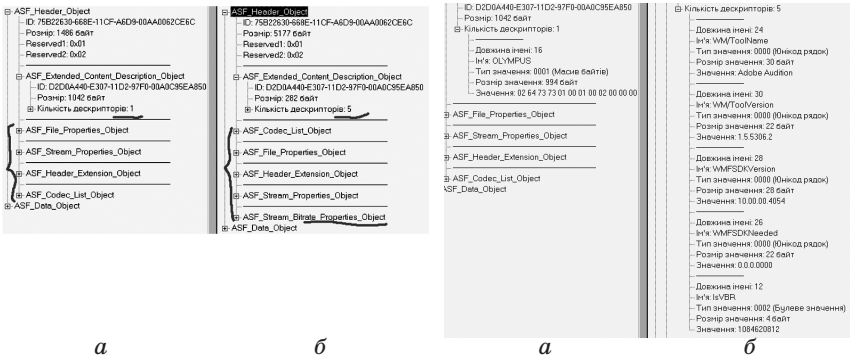
Опишемо найголовніші з блоків докладніше. Заголовок має дуже просту структуру та складається з трьох полів: кількість збережених блоків нижчого рівня та два зарезервованих, значення яких мають дорівнювати 1 та 2 відповідно.

Блок з характеристиками файлу містить інформацію з унікальним ідентифікатором файлу, розміром, датою створення, кількістю пакетів даних, часом записування, прапорами, максимальним бітрейтом та ін. Інформація є комбінованою з даних усіх потоків файлу, тому для отримання більш коректних даних стосовно кожного з них використовується блок потоку (один блок для одного потоку у файлі), який містить дані про тип потоку (аудіо-, відеотощо), корекцію помилок, проміжок часу з початку файлу, прапори та специфічні для типу потоку та корекції помилок дані.

Блок опису змісту файлу містить поля з назвою треку, ім'ям автора, авторськими правами, описом треку та його рейтингом. Уся інформація зберігається в текстовому вигляді. Для додаткових даних, які можуть знадобитися, потрібно використовувати блок

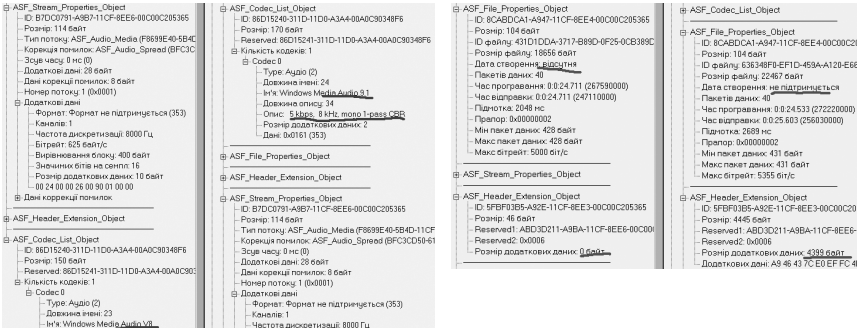
розширеного змісту, який може зберігати поля довільного типу. Для цього використовуються так звані дескриптори, а сам блок зберігає їхню кількість. Кожен дескриптор складається з текстового імені, коду типу даних (текст, масив, 2–4–8 байтове число) і самих даних.

Розглянемо структуру докладніше одночасно з аналізом змінень після редагування. Як бачимо на рис. 3, програмою Adobe Audition додаються при редагуванні 4 розширені дескриптори змісту та блок бітрейту потоку, змінюється порядок блоків у заголовку. Видно, що дескриптор з ім'ям OLYMPUS видалено, а замість нього записано п'ять інших (рис. 3). Серед характеристик аудіопотоку (рис. 4) не відбулося ніяких змінень, але відредагований файл закодовано більш новою версією кодека. Крім того, слід звернути увагу на те, як по-різному сформовано опис кодека.



а *б* *а* *б*

Рис. 3. Вікно даних файлу формату *.wma, оригінального (*а*) і відредагованого звуковим редактором Adobe Audition (*б*)



а *б* *а* *б*

Рис. 4. Вікно даних файлу формату *.wma, оригінального (*а*) і відредагованого звуковим редактором Adobe Audition (*б*)

У характеристиках файлу відбулося тільки одне змінення, яке на перший погляд придатне для виявлення редагування: додалася дата створення файлу – це поле, наприклад, цифровий диктофон Olympus WS100 залишає пустим. Змінення максимального бітрейту потребує більш ретельного вивчення. Якщо він виходить за межі діапазону бітрейтів, що підтримуються записуючим пристроєм, – це одна з ознак редагування файлу.

Як вбачається з наведеного опису форматів, а також практичного застосування програмного продукту AudioAnalizer, виявлення ознак редагування звукозаписів, виготовлених за допомогою цифрових диктофонів, подальше вдосконалення розробки, більш глибоке вивчення особливостей запису форматів звукових файлів кожним з них є нагальною потребою експертної практики. Подальше вдосконалення програмного продукту AudioAnalizer дасть можливість отримати інструмент, що серед інших відомих засобів вирішить питання дослідження ознак монтажу цифрових звукозаписів, прискорить виконання практичної експертної роботи.