Видеореги­стратор как объект исследования судебных экспертиз

С.А. Крутов^{1,2}

¹ Федеральное бюджетное учреждение Российский федеральный центр судебной экспертизы при Министерстве юстиции Российской Федерации, Москва 109028, Россия

² ФГАОУ ВО «Российский университет дружбы народов», Москва 117198, Россия

Аннотация. Рассмотрены вопросы, связанные со стационарными видеореги­страторами: их виды, назначение, принцип работы, конструктивные особенности и основные компоненты, установленные в данных устройствах. Разобран порядок использования записей с камер видеонаблюдения в судопроизводстве. Обоснована необходимость проведения комплексных экспертиз при исследовании стационарных видеореги­страторов, показано, в каких случаях необходимо назначение экспертизы, а когда достаточно осмотра с участием специалиста. Представлена последовательность исследования стационарного видеореги­стратора как объекта судебной компьютерно-технической экспертизы. Перечислены возможные вопросы к эксперту, методы и подходы; рассмотрены трудности, возникающие в ходе экспертизы. Разобран пример исследования стационарного видеореги­стратора из экспертной практики лаборатории судебной компьютерно-технической экспертизы ФБУ РФЦСЭ при Минюсте России.

Ключевые слова: *судебная компьютерно-техническая экспертиза, видеореги­стратор, накопитель на жестких магнитных дисках, видеозапись, файловая система, анализ данных в секторах, видеофайл*

Для цитирования: Крутов С.А. Видеореги­стратор как объект исследования судебных экспертиз // Теория и практика судебной экспертизы. 2021. Т. 16. № 1. С. 114–123.

<https://doi.org/10.30764/1819-2785-2021-1-114-123>

Video Recorder as an Object of Forensic Expert Analysis

Sergei A. Krutov^{1,2}

¹ The Russian Federal Centre of Forensic Science of the Ministry of Justice of the Russian Federation, Moscow 109028, Russia

² Peoples' Friendship University of Russia (RUDN University), Moscow 117198, Russia

Abstract. The article addresses the issues related to stationary video recorders: their types, purpose, principles of functioning, design characteristics, key components installed in these devices. The author analyses the procedure for using the video recordings from the surveillance cameras in court proceedings. He also justifies the need for comprehensive examinations when investigating stationary video recorders and points out the cases when the appointment of an examination is necessary and when a specialist inspection is enough. The paper presents a research sequence for a stationary video recorder as a computer forensics' object. Possible questions to the expert, methods, and approaches are listed; difficulties arising during the examination are considered. The author analyzes a case study of a stationary video recorder examination from the expert practice of the laboratory of computer forensics of the Russian Federal Centre of Forensic Science of the Russian Ministry of Justice.

Keywords: *computer forensics, video recorder, HDD, video recording, filesystem, data analysis in sectors, video file*

For citation: Krutov S.A. Video Recorder as an Object of Forensic Expert Analysis. *Theory and Practice of Forensic Science*. 2021. Vol. 16. No. 1. P. 114–123. (In Russ.).

<https://doi.org/10.30764/1819-2785-2021-1-114-123>

Введение

Видеореги­стратор представляет устройство, предназначенное для записи, хранения и воспроизведения видеоинформации (видеофайлов). Видеореги­страторы достаточно популярны, они используются не только в промышленных целях, но и в быту. Благодаря большому выбору, доступности и относительно умеренной цене, видеореги­страторы становятся выбором многих людей, которые хотят организовать видеонаблюдение в офисе, магазине, загородном доме, квартире или на предприятии.

Системы видеонаблюдения устанавли­вают на промышленных, военных объектах, активно используют в городской среде, в том числе для фиксации правонарушений, обеспечения безопасности объектов инфраструктуры города. Записи с камер могут использоваться при рассмотрении уголовных или гражданских дел, поскольку современные видеосистемы способны идентифицировать человека по характерным признакам, что помогает следователям в поимке лиц, подозреваемых в совершении того или иного преступления. Росту популярности видеореги­страторов у населения поспособствовал и тот факт, что записи с камер стали принимать суды в качестве доказательств противоправных действий – будь то кража, хулиганство, проникновение на запрещенную или частную территорию и т. п.

Использование видеоматериалов в качестве доказательств

Приобщение записей с камер видео­наблюдения сторонами по делу в качестве доказательств при рассмотрении в судах дел об административных правонарушениях стало возможным после вступления в силу Федерального закона № 114-ФЗ¹. До принятия поправок решение о необходимости приобщения данных материалов к делу оставалось за судом.

В Уголовно-процессуальный кодекс Российской Федерации (УПК РФ), Арбитражно-процессуальный кодекс Российской Федерации (АПК РФ) и Гражданско-процессуальный кодекс Российской Федера-

ции (ГПК РФ) указанные поправки пока не вносились, и это означает, что в данных кодексах действуют ранее введенные правила приобщения видеоматериала в качестве доказательств (ст. 64 и 89 АПК РФ, п. 1 ст. 55 ГПК РФ, п. 2 ст. 84 УПК РФ) – эти решения принимают правоохранительные органы или суд [1, 2].

Типы видеореги­страторов

Сегодня на рынке представлено большое количество видеореги­страторов разных производителей и с разным набором функций. В целом их можно разделить на следующие группы.

1. Сетевой стационарный видеореги­стратор. В устройстве данного типа используются IP-видеокамеры – цифровые видеокамеры, которые передают видеопоток в цифровом формате по локальной сети или сети Ethernet с использованием протокола передачи данных IP (каждой камере присваивается свой IP-адрес).

2. Гибридный стационарный видеореги­стратор. Видеореги­страторы данного типа могут работать как с аналоговыми, так и с IP-видеокамерами. Аналоговая видеокамера – устройство, предназначенное для преобразования оптического изображения в аналоговый видеосигнал, для чего используются специальные интегральные микросхемы, так называемые ПЗС-матрицы, – микросхемы из светочувствительных фотодиодов, выполненных на основе кремния, и использующие технологию управляемого переноса заряда в объеме полупроводника.

3. Система видеонаблюдения на основе персонального компьютера с платой захвата и обработки видеосигнала и подключенными к данной плате камерами.

4. Стационарный видеореги­стратор, работающий только с аналоговыми видеокамерами.

В отдельную группу можно выделить так называемые автомобильные видеореги­страторы, а также IP-видеокамеры (например, для наблюдения за ребенком из соседней комнаты). Их исследование, как правило, сводится к анализу установленной в них карты памяти формата SD (microSD), отформатированной в файловую систему FAT32 или exFAT.

Остановимся более подробно на стационарных видеореги­страторах.

¹ Федеральный закон от 26 апреля 2016 г. № 114-ФЗ «О внесении изменения в статью 26.7 Кодекса Российской Федерации об административных правонарушениях в части обязательности отнесения материалов фото- и киносъемки, звуко- и видеозаписи к доказательствам по делу об административном правонарушении» // Российская газета. 27 апреля 2016 г. № 90 (6958).

Конструктивные особенности стационарных видеорегистраторов

Стационарный видеорегистратор – это электронное устройство, сходное по строению с компьютером. В его состав входят: аналого-цифровой преобразователь, процессор, постоянная и оперативная память, устанавливаемый отдельно накопитель на жестких магнитных дисках (НЖМД) и другие компоненты. Для управления функциями видеорегистратора в его постоянной памяти записана микропрограмма. Многие видеорегистраторы могут подключаться к компьютерной сети для передачи видеоизображений на удаленные компьютеры.

Основной принцип работы видеорегистратора заключается в следующем. Видео сигнал поступает от камеры видеонаблюдения, обрабатывается процессором и сохраняется в виде видеопотока на установленном НЖМД. В случае использования аналоговых камер необходимо преобразование сигнала, за что отвечает аналого-цифровой преобразователь. Сохраненный видеопоток можно затем преобразовать в видеофайл и отправить его на удаленный компьютер или резервный носитель информации. Средствами программного обеспечения самого видеорегистратора возможен просмотр видеопотоков, в том числе удаленно с использованием компьютера или даже мобильного телефона.

Видеорегистратор как объект исследования комплексных экспертиз

Появление новых объектов или техническое усовершенствование уже существующих приводит к необходимости доработки имеющихся или разработке новых подходов к их исследованию. На сегодняшний день потребность следственных органов и судов в проведении исследования компьютерных средств достаточно высока, что в первую очередь связано с популярностью этих средств – сейчас они стали не только значимой частью нашей повседневной жизни (смартфоны, ноутбуки, видеорегистраторы), но и используются при совершении различных преступлений.

Аппаратные и программные возможности современных компьютерных систем позволяют видоизменять информацию внутри видеофайлов или файлов графических форматов, что может поставить под сомнение подлинность источников происхождения данных файлов. В этой связи возрастает ак-

туальность исследований видеофайлов на предмет монтажа. И эта задача относится к компетенции экспертов в области криминалистической экспертизы видео- и звукозаписей (КЭВиЗ)².

При решении вопроса о монтаже на экспертизу может быть предоставлен носитель информации (флэш-накопитель, оптический диск или НЖМД), содержащий только необходимые для исследования файлы. Но может быть предоставлен и носитель, ранее установленный в какой-либо компьютерной системе, например, в видеорегистраторе или персональном компьютере. В этом случае, помимо искоемых файлов или видеозаписей, носитель информации будет содержать и иные данные, в том числе других форматов. Тогда до решения основного вопроса (поиска признаков монтажа в видеофайлах) сначала необходимо найти интересные файлы или видеозаписи. Решение этой задачи уже выходит за рамки КЭВиЗ: поиск файлов определенных категорий или видеозаписей, например за конкретный промежуток времени, решается в рамках судебной компьютерно-технической экспертизы (СКТЭ). Таким образом, при решении вопроса о монтаже проведение только КЭВиЗ может быть недостаточным – потребуется привлечение эксперта-компьютерщика.

Существует ряд иных вопросов, в частности о метаданных файлов, дате записи на носитель информации, изменении системного времени компьютерного средства, которые относятся к СКТЭ. Эти вопросы следственные органы также могут ставить перед экспертами наряду с вопросом о внесении изменения в содержимое файла (монтаже) [3–7].

Потребность в привлечении эксперта для проведения компьютерно-технического исследования нередко возникает при производстве лингвистических или психологических экспертиз. В этом случае задачи будут аналогичны тем, что могут возникнуть в ходе КЭВиЗ, – это определение метаданных файлов, поиск определенных категорий файлов и т. д. [8].

Таким образом, научно-технический прогресс в области компьютерной техники, популярность и частота использования электронных устройств в повседневной

² Было отмечено, что большинство имеющихся публикаций по исследованиям записей с камер видеонаблюдения относится не к судебной компьютерно-технической экспертизе, а к КЭВиЗ.

жизни определенным образом повлияли и на судопроизводство, а также на судебную экспертизу. Все чаще для решения тех или иных задач при различных исследованиях требуется привлекать экспертов в области компьютерной техники, появилась необходимость в проведении комплексных экспертиз с обязательным участием экспертов СКТЭ.

Видеореги­стратор как объект исследования СКТЭ

Как было показано ранее, а также в связи с конструктивными особенностями и принципом работы рассматриваемых устройств, любой из представленных сегодня на рынке стационарных видеореги­страторов прежде всего является объектом компьютерно-технической экспертизы.

Изучение вопросов, связанных с исследованием стационарных видеореги­страторов, входит в программу дополнительной профессиональной подготовки государственных судебных экспертов системы Минюста России по специальности 21.1 «Исследование информационных компьютерных средств». Эти вопросы рассматриваются также при проведении стажировок, семинаров, курсов повышения квалификации государственных судебных экспертов.

Исходя из статистики ФБУ РФЦСЭ при Минюсте России, экспертизы по исследованию видеореги­страторов по сравнению с иными экспертизами, объектами исследования которых являются, например мобильные телефоны или персональные компьютеры, назначаются достаточно редко. Основной причиной этого является простота эксплуатации и получения видеоинформации с данных устройств: чтобы просмотреть записи с камер видеонаблюдения в большинстве случаев не нужны специальные знания в области компьютерной техники. Многие стационарные видеореги­страторы конструктивно и программно рассчитаны на обычных пользователей. Таким образом, следователь в ходе выемки или проведения осмотра видеореги­стратора может получить необходимые ему записи с камер видеонаблюдения с участием технического специалиста. И тогда необходимость в привлечении эксперта к решению задачи получения видеозаписи отпадает.

Однако может получиться, что при осмотре необходимой видеозаписи среди прочих не окажется, или она будет повреждена, или будет поврежден сам видеореги-

стратор или носитель информации. В этом случае следователю потребуется не только специалист, обладающий специальными знаниями в компьютерной технике, но и специализированное программное обеспечение для анализа структур файловых систем и видеозаписей видеореги­стратора. У технического специалиста, принимающего участие в выемке или осмотре, имеется достаточно знаний в области компьютерной техники, но зачастую не хватает специализированных средств, поэтому следователю для выявления всех обстоятельств дела необходимо изымать видеореги­стратор и обращаться в экспертную организацию. Кроме того, лишь судебной экспертизе присуща процессуальная форма, гарантирующая соблюдение интересов всех участников судопроизводства, а также достоверность выводов эксперта [9–12].

Особенности исследования видеореги­страторов в рамках СКТЭ

Основной задачей при исследовании видеореги­страторов в рамках судебной компьютерно-технической экспертизы является поиск записей с камер видеонаблюдения, в том числе за указанный промежуток времени. Затем эти видеозаписи нужно сохранить в виде файлов, скопировать их и предоставить лицу или органу, назначившему исследование. При этом важно, что видеозаписи необходимо предоставить в «читаемом» виде, т. е. видеофайлы нужно сохранить в известном формате (например, в расширении .avi), чтобы следователь или суд смогли просмотреть их на любом устройстве.

Вопросы, которые могут ставиться следователем или судом при проведении исследования стационарного видеореги­стратора, могут звучать так.

– Имеются ли на представленном на исследование видеореги­страторе записи с камер видеонаблюдения?

– Имеются ли на представленном видеореги­страторе записи с камер видеонаблюдения за следующий промежуток времени <указывается необходимый временной промежуток>?

Может быть поставлен и ряд других вопросов относительно информации из системного журнала видеореги­стратора или удаленных видеозаписей. Что касается удаленных файлов, то в алгоритме работы любого видеореги­стратора заложена цикличность. Это означает, что по мере заполнения

памяти носителя информации, установленного в видеорегистратор, более ранние записи с камер видеонаблюдения удаляются, и на их место записываются новые. Восстановление удаленных таким образом видеозаписей не представляется возможным.

Основной спецификой видеорегистраторов, которая может вызвать определенные трудности, является файловая система носителей информации – НЖМД, на котором размещаются видеозаписи. Данная файловая система создается средствами самого видеорегистратора при инициализации НЖМД в видеорегистраторе, а точнее средствами его операционной системы. Большинство специализированного программного обеспечения, используемого при производстве СКТЭ, не способно идентифицировать и прочесть файловые системы стационарных видеорегистраторов. Более того, в алгоритме работы данных программ вообще не предусмотрена работа с файловыми системами почти всех ныне существующих стационарных видеорегистраторов, что объясняется самобытностью этих файловых систем и их редкостью. Тем не менее некоторые разработчики программного обеспечения создали программы для исследования НЖМД видеорегистраторов, например, программу DVD Examiner. В некоторых случаях можно идентифицировать файловую систему НЖМД видеорегистратора в операционной системе Linux на стендовом компьютере эксперта.

Таким образом, основной подход к исследованию видеорегистраторов на сегодняшний день сводится к следующему. Из видеорегистратора извлекают НЖМД и при помощи соответствующего оборудования или программного обеспечения (например, аппаратно-программных комплексов Tableau TX1 или PC-3000 Portable III) создают его клон. Клон НЖМД устанавливают в видеорегистратор. После этого видеорегистратор с установленным клоном НЖМД включают и средствами его операционной системы проводят поиск, конвертацию и выгрузку искоемых видеозаписей.

Другим способом является использование «плееров», соответствующих каждому типу, а точнее производителю видеорегистраторов. Данные «плееры» представляют собой программное обеспечение, разработанное производителем видеорегистратора и предназначенное для работы с видеозаписями, создаваемыми средствами именно этого видеорегистратора. У каж-

дого производителя свой «плеер». Использование «плеера» другого производителя в большинстве случаев не приведет к желаемому результату, т. е. доступу к видеозаписям.

Трудности могут доставлять видеорегистраторы, в которых нельзя воспроизвести видеозапись с помощью «плееров». Данную функцию может не включить производитель, или может отсутствовать сам «плеер». К примеру, если в видеорегистраторе реализованы лишь функции сохранения видеопотока на установленный НЖМД и отправки видеозаписей на удаленный компьютер по локальной сети или через сеть Интернет, то эксперту при исследовании необходимо воспроизвести эти настройки, что не всегда возможно (нет необходимого дополнительного оборудования от видеокомплекса, существует риск внесения изменения в системные настройки видеорегистратора, отсутствуют знания о тонкостях настройки конкретной видеосистемы). Кроме того, установленный в стационарный видеорегистратор НЖМД может иметь логические повреждения структуры данных. В этом случае операционная система видеорегистратора может не распознать НЖМД, частично или полностью не отобразить имеющиеся видеозаписи.

Пример из экспертной практики

Рассмотрим более подробно ход производства СКТЭ³, объектом которой стал стационарный видеорегистратор, поступивший на исследование в лабораторию судебной компьютерно-технической экспертизы ФБУ РФЦСЭ при Минюсте России. Экспертиза проводилась по уголовному делу, являлась повторной и была назначена судом. На разрешении эксперта стоял вопрос: «Имеются ли на представленном на исследование видеорегистраторе видеозаписи?».

При исследовании использовали рабочее место в следующей комплектации:

- аппаратная конфигурация – процессор Intel® Core™ i7-7700;
- системная плата ASUS H170 Pro; ОЗУ 32 Гб;
- SSD-накопитель объемом 250 Гб;
- НЖМД: Western Digital объемом 2000 Гб, Seagate объемом 750 Гб, Seagate объемом 1500 Гб;
- блокирующее запись информации на НЖМД устройство Tableau;

³ Экспертизу проводил автор статьи.

– аппаратно-программный комплекс Tableau TX1 – устройство, предназначенное для снятия образа или клонирования носителей информации с интерфейсами подключения SATA и USB (разъемы для подключения источников, т. е. объектов исследования, имеют блокировку от записи).

Использовали следующую программную конфигурацию:

- операционная система Windows 10 Pro;
- аппаратно-программный комплекс PC-3000 Express, предназначенный для работы с накопителями на жестких магнитных дисках, имеющих физические и логические повреждения;
- программа Any Video Converter, предназначенная для работы с видеофайлами;
- программа DVR Examiner, предназначенная для работы с носителями информации, устанавливаемыми в стационарные видеорегистраторы.

Ход исследования.

На первоначальном этапе проводили осмотр упаковки видеорегистратора и ее фотосъемку. Затем осматривали сам видеорегистратор, при этом из корпуса видеорегистратора был извлечен НЖМД. При помощи аппаратно-программного комплекса Tableau TX1 создали побитовую копию (клон) НЖМД видеорегистратора. Клон НЖМД установили обратно в видеорегистратор.

При включении видеорегистратора⁴ и загрузки его системы управления устано-

вили, что НЖМД-клон распознается системой, но видеозаписей при этом не имеется.

В результате изучения с использованием шестнадцатеричного редактора (HEX-редактора), входящего в состав аппаратно-программного комплекса PC-3000 Express, структуры НЖМД-клона установили, что на нем имеются данные, относящиеся, вероятно, к видеозаписям. При этом схожая структура имелась практически по всему объему секторов НЖМД (рис. 1), за исключением некоторых начальных секторов, отведенных под нужды файловой системы.

Изучение инструкции по эксплуатации видеорегистратора на официальном сайте разработчика показало, что представленная на исследование модель конвертирует видеозаписи в формат .avi непосредственно средствами самого видеорегистратора, соответствующего «плеера» не имеет. В результате исследования НЖМД средствами программы DVR Examiner установили, что программа идентифицирует носитель информации, определяет тип его файловой системы, но не может получить доступ к имеющимся на НЖМД видеозаписям. Таким образом, провести информационное исследование НЖМД видеорегистратора средствами самого видеорегистратора, а также имеющимися в распоряжении у эксперта программными средствами, предназначенными для работы с носителями информации видеорегистратора, не представляется возможным.

Одним из способов решения поставленного вопроса может быть попытка понять логику размещения видеозаписей в сектора НЖМД – каким образом и по какому ал-

0x010	89 A6 E7 5F F0 4B 0F 91 65 9B 7E 7F C7 88 80 35	..._.K^..e.~i^...5
0x020	2E BD 67 3B FB BE FA 0F E0 41 FD F8 F5 AF 9B 94	..g:....^..A.....
0x030	B8 EB 47 8B 83 3C AF A4 01 2D 32 6E A5 FF 37 0D	..G..<....-2n...7.
0x040	CF A8 08 EF 5D 4F 5D 78 8B 54 64 A6 7B AE 12 A2	]0]x.Td.{...
0x050	A4 92 53 E7 C4 74 86 5A FA 5C D1 FC 11 46 E5 6E	..S...t.Z.\...F.n
0x060	24 8B AB BB 32 F5 C4 51 C6 48 BB 31 92 E2 D7 E1	\$...2...Q.H.1....
0x070	4B AD D7 F4 E4 C6 6E D9 88 97 54 2A 90 C7 B7 6C	K.....n...T*...l
0x080	15 59 CD 9A 77 8D B5 40 EC EC 19 B3 2C BE 9F 99	\$Y...w...@.....
0x090	BC B6 CF 5C 12 51 AA 5E F8 24 A8 CF 77 F8 23 D6	...\.Q.^.\$..w.#.
0x0A0	92 57 F8 22 B4 94 83 2F 7D D5 2F D5 BE AF 27 17	.W.".../}.//...'
0x0B0	C8 68 74 06 15 47 B5 E0 9F C1 22 9B CD 49 9D E9	.ht.\$G...."....I..
0x0C0	FE 32 9B 07 CF 0D 43 64 7C 99 8F B9 FF 09 78 3F	.2....Cdx?
0x0D0	BF 42 F2 52 46 49 91 95 1B 8B F1 DF 01 84 6C 07	.B.RFI.....l.
0x0E0	D2 90 E7 BF 92 F2 FF 52 26 3E 8E 7D EB 49 1A 90	R&>..}.I..
0x0F0	31 56 DC DA 2F F6 D3 60 DF EB AE 5F 5C AB 0A 4A	1V.../...`..._\...J
0x100	76 8E 83 1E 68 1D 56 D2 47 C8 30 D9 24 BF 83 4F	v...h.V.G.0.\$..0
0x110	1C F6 59 65 B2 FF D9 7F 27 48 65 85 68 C8 9A 2D	..Ye...I'He.h...-
0x120	82 22 9B CE 84 C1 5D 4B 33 04 FB 38 0D 3B 8F E9	..".....]K3...8...;

Рис. 1. Структура данных на НЖМД исследуемого видеорегистратора
Fig. 1. Data structure on the HDD of the investigated video recorder

Рис. 2. Графическое представление секторов НЖМД
Fig. 2. Graphic representation of an HDD's sectors

Рис. 3. Графическое представление примера записи информации на НЖМД видеорегистратором
Fig. 3. Graphic representation of an example of data record on an HDD by a video recorder

горитму система видеорегистратора записывала данные на НЖМД.

Для этого вновь использовали HEX-редактор из состава аппаратно-программного комплекса PC-3000 Express, средствами которого проводили анализ данных в секторах с целью поиска подобию структуры, т. е. определенной логики в построении данных.

Стоит отметить, что данный процесс может быть достаточно трудоемким и затратным по времени. В рассматриваемом примере размер одного сектора составлял 512 байт. Таким образом, для исследуемого НЖМД объемом в 250 Гб, количество секторов составляло $25\,000\,000\,000/512$ – около 500 000 000. (рис. 2), каждый из которых необходимо было просмотреть, чтобы понять, где начинаются и где заканчиваются видеопотоки.

Такая задача кажется непосильной, и ее решение отнимет много времени. Поэтому предположили, что сам видеорегистратор, хоть и является неким подобием компьютера, но не относится к устройству, способному на сложные операции, ввиду слабого по производительности процессора, небольшого объема постоянной и оперативной памяти. В совокупности с изложенным выше, а также принципом цикличности записи, можно допустить, что запись всегда начинается с начальных секторов диска (исключая сектора, занимаемые файловой системой и прочими служебными данными) и идет последовательно к конечным секторам. При заполнении всех секторов, запись начинается снова с начальных секторов, и далее – по кругу (рис. 3).

```

0x180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x190 00 00 00 00 00 00 00 00 48 59 41 56 FC 01 00 08 ..... HYAV .....
0x1A0 D4 06 97 03 D3 1D 00 00 A2 E3 9E 48 C0 1F D1 99 .....H....
0x1B0 00 00 00 00 00 00 00 00 00 00 00 01 41 9B 28 3D .....A.(=
0x1C0 E8 91 92 4F F7 19 67 3B 29 46 F7 50 D0 3E 43 A0 ...O..g;)F.P.>C.
0x1D0 A8 21 87 C9 A2 7C 10 18 4E 96 98 9C 04 C1 C6 76 .!...|..N.....v
0x1E0 6B 22 3D 3C 2D 1A 1F E3 E3 3B A5 42 47 31 04 F0 k"=<-....;..BG1..
0x1F0 6E 98 61 69 8F E3 B4 F0 21 E7 E2 04 3C 19 97 17 n.ai....!...<...

```

Рис. 4. Структура данных на НЖМД исследуемого видеорегистратора (начало контейнера)

Fig. 4. Data structure on the HDD of the investigated video recorder (beginning of the container)

```

0x0E0 04 9D B6 F1 BF 51 D4 11 B6 DC A0 86 EC 20 F9 77 .....Q..... .w
0x0F0 E8 BF D3 25 0C 9D 2A 16 5D 31 9D CB 52 60 F5 35 ...%..*.]1..R'.5
0x100 79 98 C8 64 7E 3C 95 6A 52 90 41 E9 FF A2 19 D6 y..d~<.jR.A.....
0x110 5B 1B A1 1D 47 04 77 D8 67 C0 45 68 79 61 76 7D [...G.w.g.Ehyav}
0x120 24 00 00 48 59 41 56 F0 00 00 04 66 5B 1F 01 24 $. HYAV .....f[.$.
0x130 08 00 00 A2 E3 9E 48 E7 20 D1 99 83 01 10 02 B5 .....H. ....
0x140 F7 CB F7 E2 F7 C4 F7 C1 F7 E3 F7 D6 F7 AA F7 AF .....

```

Рис. 5. Структура данных на НЖМД исследуемого видеорегистратора (окончание контейнера)

Fig. 5. Data structure on the HDD of the investigated video recorder (end of the container)

Таким образом, в процессе анализа секторов в начале НЖМД была найдена структура, похожая на начало контейнера (рис. 4).

Посекторный анализ позволил определить окончание этого контейнера (рис. 5) и следующий за ним ряд пустых секторов, а затем опять похожую на начало контейнера структуру.

Поскольку стали известны сектора размещения начала и окончания контейнера с предполагаемой видеозаписью, средства аппаратно-программного комплекса PC-3000 Express позволили выделить этот фрагмент и сохранить его на компьютере эксперта в виде файла.

В результате подбора соответствующего кодека (для большинства стационарных видеорегистраторов используется способ сжатия видеопотока в формат H.264) удалось запустить сохраненный файл на стендовом компьютере эксперта. Данный файл содержал запись с камеры видеонаблюдения. Для удобства просмотра файл с видеозаписью средствами программы Any Video Converter был перекодирован в формат .avi.

Дальнейший поиск и извлечение остальных видеозаписей проводили аналогичным образом.

Таким образом, в результате исследования видеорегистратора были найдены необходимые видеофайлы. Сложность и необычность данного подхода заключалась прежде всего в специфике файловой системы НЖМД видеорегистратора и отсутствии

универсального программного обеспечения для его исследования. Однако, предложенный метод хоть и сложнее, но позволяет более детально разобраться в ситуации и, как следствие, провести более полное исследование. Еще один аргумент в пользу данного метода заключается в том, что программа при анализе видеопотока может пропустить файл с отсутствующим окончанием. Такая ситуация может возникнуть при внезапном отключении питания видеорегистратора. «Ручной» метод позволит увидеть и в некоторых случаях восстановить целостность «недописанного» файла путем добавления в его структуру окончания. Данная процедура не будет являться изменением файла, поскольку не затрагивает его пользовательские данные, а лишь восстанавливает его целостность путем добавления системных данных.

Заключение

Приведенное исследование показало, что существующие подходы к исследованию стационарных видеорегистраторов сводятся лишь к извлечению информации средствами самих видеорегистраторов или их программного обеспечения. С одной стороны, для решения большинства задач, связанных с данными объектами исследования, этого достаточно, но с другой – существующий подход не учитывает сторонних факторов, связанных с физическим разрушением объекта исследования, будь то сам видеорегистратор или установленный в

него носитель информации. Как следствие, задача получения видеозаписи при наличии физических повреждений становится практически нерешаемой [13–15].

На сегодняшний день в ФБУ РФЦСЭ при Минюсте России был применен новый способ исследования стационарного видеорегистратора, что позволило решить поставленную перед экспертом задачу – поиск и

сохранение видеофайла. Дальнейшее изучение структуры размещения видеозаписей на НЖМД видеорегистраторов различных марок, моделей и производителей позволит установить, является ли данный подход универсальным, и возможно ли его применение в дальнейшем уже в статусе рекомендованного к широкой экспертной практике.

СПИСОК ЛИТЕРАТУРЫ

1. Талынева З.З., Давыдова С.Р. К вопросу о доказательственном значении материалов аудио- и видеозаписи в уголовном процессе // Вестник Уфимского юридического института МВД России. 2018. № 4 (82). С. 54–57.
2. Россинский С.Б. Приложение к протоколу следственного действия: признавать или не признавать как вещественное доказательство? // Вестник Восточно-Сибирского института МВД России. 2017. № 2 (81). С. 94–104.
3. Воронкова Д.К., Воронков А.С., Пилипчак А.М. Комплексная судебная компьютерно-техническая и видеотехническая экспертиза // Modern Science. 2019. № 12-1. С. 300–306.
4. Эджузов Л.Г., Усов А.И., Микляева О.В. Новая концепция и существующее представление о комплексной судебной экспертизе // Теория и практика судебной экспертизы. 2014. № 2 (34). С. 142–149.
5. Эджузов Л.Г., Усов А.И., Микляева О.В., Карпухина Е.С. О месте новой концепции в теории комплексной экспертизы // Теория и практика судебной экспертизы. 2014. № 2 (34). С. 10–17.
6. Вознюк М.А., Денисов Ю.А. Экспертная диагностика обстоятельств изготовления цифровых видео- и звукозаписей: аналитический обзор // Теория и практика судебной экспертизы. 2017. Т. 12. № 1. С. 48–71. <https://doi.org/10.30764/64/1819-2785-2017-12-1-48-71>
7. Хатунцев Н.А., Лизоркин А.М. Метод доказывания неизменности фотоизображений в рамках компьютерно-технической экспертизы (на примере из экспертной практики) // Теория и практика судебной экспертизы. 2014. № 3 (35). С. 69–73.
8. Бондарев А.А., Кривенок А.М., Кузнецов В.О. Применение методов СКТЭ и КЭЗ при решении вопроса о датировке видеофонограммы и наличии/отсутствии признаков ее монтажа и изменения // Теория и практика судебной экспертизы. 2011. № 2 (22). С. 124–126.
9. Усов А.И. Судебно-экспертное исследование компьютерных средств и систем. Основы методического обеспечения. Учебное пособие / Под ред. Е.Р. Россинской. М.: Право и Закон, Экзамен, 2003. 368 с.

REFERENCES

1. Talyneva Z.Z., Davydova S.R. To the Question of Evidentiary Value of the Materials Audio and Video Recordings in Criminal Proceedings. *Bulletin of Ufa Law Institute*. 2018. No. 4 (82). P. 54–57. (In Russ.)
2. Rossinskiy S.B. Annex to an Investigative Proceedings Record: To Recognize or Not To Admit As Physical Evidence? *Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of the Russian Federation*. 2017. No. 2 (81). P. 94–104. (In Russ.)
3. Voronkova D.K., Voronkov A.S., Pilipchak A.M. Comprehensive Forensic Computer and Video Examination. *Modern Science*. 2019. No. 12-1. P. 300–306. (In Russ.)
4. Edzhubov L.G., Usov A.I., Miklyaeva O.V. New Concept and Current Understanding of Integrated Forensic Investigation. *Theory and Practice of Forensic Science*. 2014. No. 2 (34). P. 142–149. (In Russ.)
5. Edzhubov L.G., Usov A.I., Miklyaeva O.V., Karpukhina E.S. Introducing a New Concept in the Theory of Integrated Forensic Investigation. *Theory and Practice of Forensic Science*. 2014. No. 2 (34). P. 10–17. (In Russ.)
6. Voznyuk M.A., Denisov Y.A. Forensic Diagnostics of the Circumstances of Digital Video and Audio Production: Analytical Review. *Theory and Practice of Forensic Science*. 2017. Vol. 12. No. 1. P. 48–71. (In Russ.). <https://doi.org/10.30764/64/1819-2785-2017-12-1-48-71>
7. Khatuntsev N.A., Lizorkin A.M. Method of Proof Invariably Images in the Computer-Technical Expertise (from Expert Practice). *Theory and Practice of Forensic Science*. 2014. No. 3 (35). P. 69–73. (In Russ.)
8. Bondarev A.A., Krivenok A.M., Kuznetsov V.O. Application of Forensic Computer-Technical Expertise and Criminalistic Expertise of Sound Recordings Methods for Dating the Videophonogram and the Presence of Indices of Its Modification. *Theory and Practice of Forensic Science*. 2011. No. 2 (22). P. 124–126. (In Russ.)
9. Usov A.I. *Forensic Examination of Computer Tools and Systems. Basics of Methodological Support. Textbook* / E.R. Rossinskaya (ed). Moscow: Pravo i Zakon, Ekzamen, 2003. 368 p. (In Russ.)

10. Производство судебной компьютерно-технической экспертизы. I. Общая часть. II. Диагностические и идентификационные исследования аппаратных средств. Методическое пособие / Под редакцией А.И. Усова М.: ФБУ РФЦСЭ при Минюсте России, 2009. 80 с.
11. Momunkulov A.R., Nazarov M.A. The Theoretical Aspects of the Conducting Investigative Activity in the Cases of Cybercrimes // *Modern Science*. 2018. No. 8. P. 74–78.
12. Хатунцев Н.А. О специальных знаниях, необходимых при исследовании компьютерных средств и систем // *Актуальные проблемы российского права*. 2010. № 1 (14). С. 332–339.
13. Хатунцев Н.А., Карпукхина Е.С. Конференция ENFSI FIT WG «Информационные технологии в судебной экспертизе, 2014» // *Теория и практика судебной экспертизы*. 2015. № 1 (37). С. 112–113.
14. Van Dongen W.S. Case Study: Forensic Analysis of a Samsung Digital Video Recorder // *Digital Investigation*. 2008. Vol. 5. No. 1–2. P. 19–28. <https://doi.org/10.1016/j.diin.2008.04.001>
15. Poole N.R., Abatis Q.Z.P. Analysis of CCTV Digital Video Recorder Hard Disk Storage System // *Digital Investigation*. 2009. Vol. 5. No. 3–4. P. 85–92. <https://doi.org/10.1016/j.diin.2008.11.001>
10. Usov A.I. (ed). *Conduct of Forensic Computer Expertise. I. General Part. II. Diagnostic and Identification Examination of Hardware. Handbook*. Moscow: RFCFS, 2009. 80 p. (In Russ.)
11. Momunkulov A.R., Nazarov M.A. The Theoretical Aspects of the Conducting Investigative Activity in the Cases of Cybercrimes. *Modern Science*. 2018. No. 8. P. 74–78. (In Russ.)
12. Khatuntsev N.A. On the Specialized Knowledge Required in Examination of Computer Tools and Systems. *Actual Problems of the Russian Law*. 2010. No. 1 (14). P. 332–339. (In Russ.)
13. Khatuntsev N.A., Karpukhina E.S. ENFSI FIT WG Conference “Information Technologies in Forensic Science 2014”. *Theory and Practice of Forensic Science*. 2015. No. 1 (37). P. 112–113. (In Russ.)
14. Van Dongen W.S. Case Study: Forensic Analysis of a Samsung Digital Video Recorder. *Digital Investigation*. 2008. Vol. 5. No. 1–2. P. 19–28. <https://doi.org/10.1016/j.diin.2008.04.001>
15. Poole N.R., Abatis Q.Z.P. Analysis of CCTV Digital Video Recorder Hard Disk Storage System. *Digital Investigation*. 2009. Vol. 5. No. 3–4. P. 85–92. <https://doi.org/10.1016/j.diin.2008.11.001>

ИНФОРМАЦИЯ ОБ АВТОРЕ

Крутов Сергей Александрович – заместитель заведующего лабораторией судебной компьютерно-технической экспертизы ФБУ РФЦСЭ при Минюсте России; e-mail: serdgiob@yandex.ru

*Статья поступила: 05.01.2021
После доработки: 30.01.2021
Принята к печати: 15.02.2021*

ABOUT THE AUTHOR

Krutov Sergei Aleksandrovich – Deputy Head of the Laboratory of Computer Forensics; the Russian Federal Centre of Forensic Science of the Russian Ministry of Justice; e-mail: serdgiob@yandex.ru

*Received: January 05, 2021
Revised: January 30, 2021
Accepted: February 15, 2021*