Дата поступления рукописи в редакцию: 04.10.2026 г. DOI: 10.24412/2224-9133-2026-10-310-318
Дата принятия рукописи в печать: 10.11.2026 г.

КАСЬЯНОВ Александр Олегович,
преподаватель кафедры криминалистики учебно-научного комплекса по предварительному следствию в органах внутренних дел Волгоградской академии МВД России, майор полиции,
e-mail: masila179@yandex.ru

ТАРАН Александра Владимировна,
преподаватель кафедры уголовного процесса и криминалистики Ставропольского филиала Краснодарского университета МВД России,
e-mail: taran_aleksandra86@mail.ru

УШАКИНА Юлия Сергеевна,
старший преподаватель кафедры управления и административной деятельности органов внутренних дел Белгородского юридического института МВД России имени И.Д. Путилина, кандидат юридических наук, подполковник полиции,
e-mail: Nikjulijas@mail.ru

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ РЕЗУЛЬТАТОВ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ И ЦИФРОВЫХ МАТЕРИАЛОВ В ДОКАЗЫВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЁННЫХ В ХОДЕ МАССОВЫХ МЕРОПРИЯТИЙ

Аннотация. *Предмет исследования — уголовно-процессуальные и оперативно-розыскные отношения, возникающие при выявлении, фиксации и доказывании преступлений, совершённых во время массовых мероприятий. Цель работы — определить критерии правомерного и проверяемого включения результатов оперативно-розыскной деятельности и цифровых материалов в уголовно-процессуальное доказывание. Применены формально-юридический, системно-структурный и сравнительно-правовой методы, анализ законодательства, правовых позиций высших судов и научных публикаций. Обосновано разграничение цифровых сведений по способу их первоначального получения; выявлены риски утраты исходного файла, подмены процессуальной фиксации оперативной справкой, ошибочной идентификации лица и ограничения прав участников. Предложена модель проверяемой цифровой прослеживаемости, объединяющая установление правового основания получения материала, сохранение его происхождения и целостности, процессуальное закрепление и состязательную проверку. Сформулированы предложения по совершенствованию межведомственного порядка передачи материалов и документирования проверочных действий. Вывод: доказательственное значение цифровой записи определяется не масштабом видеофиксации, а законностью её получения, воспроизводимостью процедуры проверки и возможностью защиты оспорить содержащиеся в ней сведения.*

Ключевые слова: *уголовное судопроизводство; оперативно-розыскная деятельность; массовые мероприятия; цифровые материалы; видеозапись; допустимость доказательств; цифровая прослеживаемость; процессуальные гарантии.*

Для цитирования: *Касьянов А. О., Таран А. В., Ушакина Ю. С. Проблемы использования результатов оперативно-розыскной деятельности и цифровых материалов в доказывании преступлений, совершённых в ходе массовых мероприятий // Право и управление. 2026. № 10. С. 310–318.*

KASYANOV Alexander Olegovich,
Lecturer in the Forensic Science Department of the Preliminary Investigation Training and Research Complex in Internal Affairs Bodies at the Volgograd Academy of the Ministry of Internal Affairs of Russia, Police Major

TARAN Alexandra Vladimirovna,
lecturer of the Department of Criminal Procedure and Forensic Science of the Stavropol branch of the Krasnodar University of the Ministry of Internal Affairs of Russia

USHAKINA Yulia Sergeevna,
Senior Lecturer in the Department of Management and Administrative Activities of Internal Affairs Bodies at the I.D. Putilin Belgorod Law Institute of the Ministry of Internal Affairs of Russia, PhD in Law, Police Lieutenant Colonel

PROBLEMS OF USING OPERATIONAL-SEARCH RESULTS AND DIGITAL MATERIALS AS EVIDENCE OF CRIMES COMMITTED DURING MASS EVENTS

Annotation. *The article examines criminal procedural and operational-search relations arising from the detection, recording and investigation of crimes committed during mass events. Its purpose is to identify criteria for the lawful and verifiable use of operational-search results and digital materials in criminal proceedings. Formal legal, systemic and comparative methods are applied to legislation, judicial positions and academic literature. The study differentiates digital materials by the legal basis on which they were originally obtained and identifies risks involving loss of original files, substitution of procedural verification with operational reports, erroneous identification and restrictions on defence rights. A model of verifiable digital traceability is proposed. It combines assessment of the lawful origin of data, preservation of integrity and provenance, procedural incorporation and adversarial examination. Recommendations are made for improving interagency transfer procedures and recording verification activities. The conclusion is that the evidentiary value of digital recordings depends on lawful acquisition, reproducibility of verification and effective opportunities for the defence to challenge the information, rather than on the scale of surveillance.*

Key words: *criminal proceedings; operational-search activities; mass events; digital materials; video recordings; admissibility of evidence; digital traceability; procedural safeguards.*

For citation: *Kasyanov A. O., Taran A. V., Ushakina Yu. S. Problems of using operational-search results and digital materials as evidence of crimes committed during mass events. Law and administration. 2026; (10):310–318. (In Russ.).*

Массовое мероприятие представляет собой особую среду формирования доказательственной информации, поскольку значительное число участников, динамика перемещений, одновременная работа нескольких систем видеонаблюдения, публичность происходящего и ограниченность времени на сохранение записей создают условия, при которых обстоятельства одного события фиксируются разными субъектами и в различных правовых режимах. При этом в распоряжение следователя способны поступить записи стационарных камер, видеорегистраторов сотрудников полиции, мобильных устройств очевидцев, файлы из открытых источников, а также материалы, полученные оперативными подразделениями. По нашему мнению, вопрос о доказательственном использовании таких материалов приобретает особую остроту при расследовании причинения вреда здоровью, хищений, применения насилия в отношении представителя власти, повреждения имущества и иных преступлений, совершаемых в местах массового пребывания людей. Мы считаем, что существенно не только установить, кто совершил конкретное деяние, но и индивидуализировать действия лица, исключить смешение нескольких эпизодов и обеспе-

чить возможность проверки исходной информации, поскольку простое нахождение человека в зоне события или его присутствие в кадре само по себе не свидетельствует о причастности к преступлению.

Цель нашей статьи обосновать комплексный подход к использованию результатов ОРД и цифровых материалов в доказывании преступлений, совершённых в ходе массовых мероприятий, поскольку Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» [11] хотя и предусматривает возможность использования результатов ОРД в уголовном судопроизводстве, но статья 89 УПК РФ [12] прямо запрещает их применение, если они не отвечают требованиям, предъявляемым к доказательствам, из чего следует принципиальный вывод, что полезность оперативной информации для раскрытия преступления ещё не означает её процессуальной пригодности для обоснования обвинения. При этом необходимо отметить, что в юридической науке довольно обстоятельно обсуждаются представление результатов ОРД органам расследования [1], содержание оперативно-розыскного обеспечения уголовного судопроизводства [2], доказательственный потенциал электронно-цифровых следов [3], правовая природа электронных доказательств [4] и особенности использования видеозаписи [5]. Вместе с тем, мы считаем, что соединение указанных проблем применительно к массовым мероприятиям требует самостоятельного анализа, так как здесь одновременно действуют оперативные, процессуальные, организационные и технические факторы.

В нашей работе термин «массовые мероприятия» используется как исследовательское обобщение, включающее публичные, спортивные, культурно-зрелищные и иные события с концентрацией людей, он не подменяет специальные определения и правовые режимы, закреплённые для отдельных видов мероприятий, речь идёт не о допустимости наблюдения за всеми участниками как такового, а о правомерном обращении с конкретными сведениями при наличии относимости к событию предполагаемого преступления. В литературе так же указывается на расширение использования информационных технологий и дистанционных технических средств при охране общественного порядка на публичных и иных массовых мероприятиях [6; 7]. При этом технические системы, ориентированные на предупреждение угроз и управление потоками людей, изначально проектируются не для уголовно-процессуального доказывания и превращение их записей в материалы уголовного дела требует самостоятельных правовых действий и оценки обстоятельств возникновения файла.

И первая особенность рассматриваемой нами среды, это множественность точек наблюдения, когда один конфликт способен попасть в поле зрения камер организатора, городской инфраструктуры и персональных устройств, а записи отличаются углом съёмки, частотой кадров, разрешением, настройками часов, условиями освещения и продолжительностью. При этом отсутствие какого-либо действия в одной записи не всегда означает, что оно не имело места, так как событие могло находиться вне видимой зоны либо между отдельными кадрами.

Вторая особенность связана с высокой скоростью изменения обстановки, так как архивы некоторых систем автоматически перезаписываются, а видеоролики очевидцев оперативно размещаются в социальных сетях, редактируются и пересылаются, в связи с чем промедление с законным получением первичного файла может повлечь утрату метаданных и затруднить определение реального времени записи. И вот тут возникает необходимость своевременно устанавливать владельца системы, регламент хранения и лицо, способное предоставить исходный материал.

И, третья особенность, это вероятность ошибочной индивидуализации действий, поскольку в условиях плотного скопления людей затрудняется различение участников эпизода, особенности одежды могут повторяться, а фрагментарный видеоряд создаёт ложное впечатление причинно-следственной связи. Тут необходимо отметить, что даже при применении алгоритмов сопоставления изображений результаты распознавания необходимо оценивать критически, поскольку они являются основанием для проверки версии, но не освобождают от подтверждения личности и действий совокупностью доказательств.

Научно обоснованное решение рассматриваемой нами проблемы требует классификации материалов не по расширению файла, а по способу первоначального получения, когда можно выделить четыре группы: результаты ОРМ, содержащие цифровую информацию; записи, созданные техническими системами охраны и видеонаблюдения вне ОРД; материалы, добровольно представленные частными лицами и цифровые сведения, полученные в порядке уголовно-процессуальных действий. При этом для каждой группы неодинаковы исходные документы, основания вмешательства и последующие процедуры проверки. Первая группа охватывает сведения, полученные уполномоченными оперативными подразделениями при проведении предусмотренных законом мероприятий, к примеру наблюдения, если оно проводилось именно как ОРМ, когда применяются требования статей 6–8 и 11 Закона об ОРД, а также установленный порядок представления результатов. Тут необходимо обратить

внимание на тот факт, что наличие записи, произведённой сотрудником полиции, само по себе не делает её результатом ОРД, решающее значение имеет правовой режим соответствующего действия.

Ко второй группе относятся записи систем, функционирующих в целях организации мероприятия, обеспечения пропускного режима, общественной безопасности и сохранности имущества. При этом при отсутствии признаков проведения ОРМ такая запись не должна искусственно квалифицироваться как оперативно-розыскной результат, процессуальное значение могут приобрести сведения, представленные оператором системы, а также обнаруженные и исследованные при осмотре надлежащим образом полученные файлы и носители.

Третья группа включает в себя видеоролики очевидцев, фотографии, переписку и размещённые в интернете материалы. Мы считаем, что распространённая цепочка «оригинал — пересылка — публикация — скачивание» представляет некоторую проблему, так как она может изменить параметры файла, убрать звук, обрезать изображение или уничтожить метаданные, а сведения о публикации и сведения о событии, запечатлённом на ней, не являются равнозначными фактами и следователь в первую очередь должен выяснить автора, обстоятельства съёмки и происхождение переданного экземпляра, если они могут быть установлены.

Четвёртая же группа объединяет материалы, полученные посредством предусмотренных УПК РФ следственных и иных процессуальных действий, когда качество доказательственной информации зависит от соблюдения процессуальной формы, включая фиксацию хода и результатов осмотра, приобщение объектов в установленном порядке, обеспечение прав участников и оценку необходимости специальных знаний. Но необходимо отметить, что использование технических средств не устраняет требований статей 74, 75, 81, 84, 86–88 УПК РФ.

В Контексте нашего исследования мы считаем, что смешение перечисленных групп приводит к двум противоположным ошибкам, когда, во-первых, обычная запись с камеры получает статус «результата ОРД» без соответствующего правового основания и документов, а во-вторых, материал, фактически полученный при ОРМ, передаётся как частное видео, вследствие чего исключается проверка законности мероприятия. Предлагаемая же нами классификация, на наш взгляд, позволяет установить необходимую процедуру до решения вопроса о доказательственном использовании. Статья 11 Закона об ОРД допускает представление результатов оперативно-розыскной деятельности органу дознания, следователю или в суд, в том числе для использования в доказывании с соблюдением УПК РФ, статья 89 которого формулирует отрицательный критерий, запрещается использование таких результатов, если они не отвечают требованиям, предъявляемым к доказательствам. То есть указанные положения образуют правовой механизм, в котором оперативная информация не освобождается от процессуальной проверки.

Конституционный Суд РФ еще в определении от 4 февраля 1999 г. № 18-О [13] разъяснил, что результаты ОРМ сами по себе не являются доказательствами, а сведения об источниках фактов могут получить доказательственное значение после закрепления надлежащим процессуальным путём. В тоже время несмотря на принятие этого акта при действии прежнего уголовно-процессуального законодательства, сформулированное разграничение сохраняет принципиальное методологическое значение для оценки связи ОРД и уголовного судопроизводства.

Отметим, что в пункте 9 постановления Пленума Верховного Суда РФ от 29 ноября 2016 г. № 55 «О судебном приговоре» [14] подчёркивается необходимость соответствия ОРМ задачам, основаниям и условиям, предусмотренным Законом об ОРД, установленного порядка представления сведений и их закрепления путём соответствующих следственных либо судебных действий, в частности, видеозаписи должны быть осмотрены и приобщены к делу. А, кроме того, Пленум также указывает, что признанные недопустимыми результаты не могут быть восполнены допросом сотрудников, проводивших ОРМ.

Порядок представления результатов ОРД, в свою очередь, регламентирован межведомственной Инструкцией, утверждённой совместным приказом от 27 сентября 2013 г. № 776/703/509/507/1820/42/535/398/68, предусматривающей документы представления и требования к содержащимся сведениям [15]. И, хотя в научной литературе подчёркивается необходимость согласования интересов расследования, режима секретности и охраны лиц, содействующих оперативным подразделениям [1; 2], технические особенности цифровых приложений ставят дополнительные задачи, не исчерпываемые самим фактом передачи рапорта или постановления, особенно при расследовании преступления, совершённого на массовом мероприятии, когда следователю недостаточно констатировать наличие диска или файла в приложении к оперативным материалам, ему необходимы сведения, позволяющие проверить, в рамках какого ОРМ получена запись, кто и когда её создал или скопировал, какие изменения вносились в цифровой массив и каким образом он поступил в распоряжение следствия. Но необходимо понимать, что не всякая оператив-

ная информация подлежит раскрытию публично, имеются пределы раскрытия, определяющиеся требованиями закона и необходимостью защиты охраняемых сведений.

Следует так же различать два направления использования результатов ОРД, которые в качестве ориентирующей информации помогают выдвигать версии, устанавливать очевидцев, выбирать законные проверочные действия и определять зоны поиска иных записей, а в доказательственном аспекте информация требует проверяемого процессуального оформления и оценки допустимости. Смешение этих функций, на наш взгляд, ведёт к необоснованному переносу оперативных выводов в обвинение без независимой проверки первичного источника.

Наконец, само по себе наличие решения о проведении ОРМ ещё не подтверждает достоверность конкретного цифрового файла, законность первоначального получения и сохранность дальнейшей информационной цепочки должны исследоваться раздельно. Вот почему вопросы ограничений оперативно-розыскных мероприятий справедливо рассматриваются в научных работах как самостоятельные гарантии защиты личности и их содержание приобретает практическое значение в том числе при оценке цифровых записей массовых событий [8].

Теперь рассмотри получение материалов на стадии проверки сообщения о преступлении, как на начальной стадии расследования, когда особенно важно сочетать своевременность фиксации сведений с соблюдением процессуальных гарантий. Статья 144 УПК РФ предоставляет предусмотренные законом возможности для проверки сообщения о преступлении, а часть 1.2 названной статьи допускает использование полученных сведений в качестве доказательств при соблюдении требований статей 75 и 89 УПК РФ. Следовательно, очевидно, что проведение проверочных действий до возбуждения уголовного дела не означает автоматического исключения их результатов из доказывания, но и не обеспечивает их безусловной допустимости. Применительно же к цифровой записи целесообразно уже при первичном обращении фиксировать сведения об источнике, такие как расположение и принадлежность камеры, примерный интервал видеозаписи, особенности часов системы, известные случаи перезаписи, способ и носитель предполагаемого предоставления. Но получение этих данных не должно подменять следственные действия, требующие соблюдения специально установленной процедуры, цель первичной фиксации - это обеспечить возможность последующего законного собирания и проверки сведений.

Нередко на стадии проверки поступает короткий фрагмент, визуально подтверждающий конфликт, но отсутствие предшествующих или последующих эпизодов может менять оценку поведения участников, поэтому следует обеспечить получение более полного временного интервала и иных ракурсов, причём с соблюдением требований относимости, законности и минимизации обработки сведений о посторонних гражданах.

Недопустимо так же создавать ситуацию, при которой видеоматериал сначала анализируется вне процессуальных процедур, затем подвергается незафиксированной обработке, а на осмотр представляется только результирующий монтаж. В таком случае следователь и суд рискуют оценивать не первоначальный информационный объект, а отобранную третьим лицом интерпретацию события, ведь если обработанный фрагмент имеет ориентирующее значение, его происхождение и связь с первоисточником должны быть установлены отдельно.

При определении дальнейшей тактики следует учитывать правовой режим электронных носителей, в том числе специальные положения статьи 164.1 УПК РФ и сферы её применения, поскольку распространять предусмотренные этой нормой ограничения и исключения на любые уголовные дела без анализа условий её действия юридически неверно, предметом процессуальной оценки должны быть конкретные способ получения данных, характер носителя, основания необходимых действий и соблюдение прав затронутых лиц.

Как известно цифровой файл способен одновременно содержать визуальные сведения, звук, отметки времени, координаты, параметры кодирования и служебные метаданные, хотя наличие технических атрибутов и не гарантирует их первоначальной точности, часы регистратора могут отставать, координаты отсутствовать, а время изменения файла обновляться при копировании. Поэтому цифровая аутентификация представляет собой не одно действие, а совокупность проверок происхождения, целостности и соответствия содержания реальным обстоятельствам. В связи с чем в работах, посвящённых электронно-цифровым следам, отмечается сложность их формирования и последующей интерпретации, а исследования правовой природы электронных доказательств показывают необходимость различать информацию и её материальный либо электронный носитель [3; 4; 9]. В контексте нашего исследования, применительно к массовому мероприятию это требует фиксации не только того, что видео воспроизводится, но и источника файла, истории его копирования, применённого программного обеспечения и условий просмотра. При этом для обеспечения целостности может использоваться вычисление контрольных сумм файлов по общепринятым криптографиче-

ским алгоритмам с указанием алгоритма, даты и полученного значения в соответствующих материалах. Такая процедура, несомненно, полезна для установления идентичности экземпляров, но действующее уголовно-процессуальное законодательство не следует представлять как содержащее универсальное требование о хешировании каждого видеофайла, тут речь идёт о предлагаемой криминалистической мере, применяемой в пределах законных процедур и технических возможностей.

Обязательным содержательным вопросом, на наш взгляд, остаётся различение исходного файла, рабочей копии и аналитического продукта, так как исходный файл следует сохранять в доступном законом объёме без редактирования. Копия же может использоваться для воспроизведения и исследования, а увеличенные изображения, стабилизация, замедление и компоновка нескольких ракурсов представляют собой производные материалы, при создании которых необходимо сохранять возможность сопоставления с исходной информацией и фиксировать характер преобразований. Поскольку видеоряд не всегда позволяет надёжно установить существенные обстоятельства, короткий фрагмент может не показывать начала конфликта, закрывать действие посторонним объектом либо создавать иллюзию близости находящихся на разных планах людей. Поэтому оценку содержания записи целесообразно соотносить с показаниями, данными о расположении камер, результатами осмотра места происшествия, экспертными выводами и иными допустимыми доказательствами.

Сопоставляя цифровые материалы, необходимо учитывать и возможность непреднамеренной модификации при передаче через мессенджер или публикации в сети, так как различия разрешения, размера файла и времени его создания не во всех случаях означают фальсификацию, хотя их причины и требуют объяснения. Тем более, что для массовых мероприятий характерна фрагментация единого события между несколькими камерами. Так в одной записи может быть отражено приближение участников, в другой физический контакт, в третьей уже последствия и воссоздание временной последовательности требует установления зон видимости, синхронизации времени и обоснования того, что на разных файлах запечатлены одни и те же лица и эпизод. Механическое же размещение кадров рядом без проверки исходных параметров способно сформировать ошибочную реконструкцию.

В этой связи нам представляется целесообразным разграничивать «сведение ракурсов» как аналитическую операцию и «установление факта» как результат доказательственной оценки. Синхронизированный ролик, созданный для наглядности, не должен заменять самостоятельное исследование каждого первичного источника, в материалах дела необходимо отображать способ совмещения, использованные временные метки и пределы возможной погрешности, если эти обстоятельства имеют значение. Идентификация же лица только по изображениям требует особой осторожности, поскольку в условиях толпы одежда, головной убор и положение в пространстве представляют собой косвенные признаки и алгоритмическое совпадение изображения лица может зависеть от качества, угла съёмки и параметров системы. Но полученный программный результат целесообразно рассматривать как проверяемое информационное указание, а не замену процессуального установления личности или самостоятельное доказательство виновности.

Индивидуализация поведения имеет самостоятельное правовое значение при разграничении участников массового события и лиц, совершивших конкретные действия, так как для уголовного судопроизводства должны быть установлены признаки деяния и роль конкретного лица, а не абстрактная характеристика группы. К примеру, движение человека рядом с местом повреждения имущества не доказывает причинение повреждения, а нахождение в группе во время конфликта не подтверждает участие в насилии.

Развитие интеллектуального видеоанализа, несомненно, увеличивает скорость поиска эпизодов, выделения объектов и сопоставления изображений, однако, технология решает задачу отбора и обработки данных, а не устанавливает юридическую виновность, тем более что в контексте массовых мероприятий ошибка алгоритма может повлечь проверочные действия в отношении лица, случайно оказавшегося рядом с событием. В связи с чем каждый существенный вывод автоматизированной системы должен сохранять возможность независимой проверки человеком. Так, правовую оценку необходимо начинать с разграничения целей первоначального видеонаблюдения и последующего уголовно-процессуального использования записи, поскольку даже если материал правомерно возник в системе обеспечения безопасности, его дальнейшее копирование, распространение и анализ должны соотноситься с законными основаниями и объёмом необходимых сведений. Нельзя забывать, что публичный характер события не равнозначен неограниченному отказу каждого участника от прав на частную жизнь и защиту персональных данных.

Вопрос о допустимости материалов невозможно решить исключительно техническими средствами, поскольку конституционные гарантии неприкосновенности частной жизни, тайны сообщений и свободы собраний предполагают соблюдение закона при получении и использова-

нии сведений. Если конкретное ОРМ затрагивает конституционные права, требуется выполнение специальных условий, предусмотренных Законом об ОРД, массовость события не создаёт самостоятельного универсального разрешения на такие ограничения.

Состязательность в свою очередь предполагает реальную возможность стороны защиты проверить и оспорить доказательства обвинения, а применительно к видео это означает доступ к относящимся к делу материалам и информации, необходимой для оценки происхождения, непрерывности и полноты записи, с учётом установленных законом ограничений и демонстрация короткого фрагмента без возможности поставить вопрос об исходном источнике способна нарушить баланс процессуальных возможностей сторон.

Отдельно, на наш взгляд, следует оценивать информацию о лицах, не связанных с предметом доказывания, так как правомерная защита таких лиц достигается прежде всего обоснованным ограничением объёма собирания и обращения с материалами, а при необходимости и использованием законных мер охраны персональных сведений. При этом обезличенная или замаскированная рабочая копия не должна уничтожать возможность проверки полноценного исходного материала компетентными участниками уголовного судопроизводства.

В контексте вышеизложенного мы хотим предложить авторскую модель проверяемой цифровой прослеживаемости, или иными словами документированную последовательность юридически значимых и технических действий с цифровым материалом, позволяющую установить правомерность его получения, тождество исследуемого экземпляра, содержание процессуального закрепления и возможность последующей проверки сторонами и судом. При этом отметим, что предлагаемая модель не является новым процессуальным источником доказательств и не заменяет предусмотренные УПК РФ правила.

Итак, первый элемент модели это квалификация первоначального источника, когда устанавливается, возник ли материал при ОРМ, в системе охраны мероприятия, при частной съёмке либо в ходе процессуального действия. Фиксируются лицо или организация, способные подтвердить происхождение записи, а также правовое основание её получения и передачи. То есть на этом этапе исключается необоснованная подмена результатов ОРД материалами иной категории и обратная ошибка.

Второй элемент это сохранение исходного информационного объекта, когда по возможности определяется первоначальный носитель или первичный экземпляр записи, выделяется релевантный временной интервал, фиксируются сведения о технической системе и факте копирования. А в случае создания контрольных сумм и рабочих копий, указываются параметры процедуры. То есть, изменения оригинала по возможности исключаются, а объективные технические ограничения отражаются в документах без сокрытия.

Третий элемент предполагает процессуальное закрепление и содержательную проверку, сведения осматриваются и приобщаются в порядке, отвечающем их юридической природе, сопоставляются с иными доказательствами, исследуются вопросы точности времени, полноты эпизода и видимых действий, при необходимости привлекаются лица со специальными знаниями и результаты аналитической обработки не смешиваются с первичным файлом.

И, наконец, четвёртый элемент - состязательная проверяемость, означающая, что стороны должны обладать предусмотренными законом возможностями поставить вопрос о происхождении файла, наличии обрезки, качестве изображения, ошибке синхронизации, альтернативной интерпретации поведения и пределах применённого программного анализа. То есть, материалы, на которых строится обвинение, должны быть доступны для судебной оценки в допустимом законом режиме, так как ограничение доступа требует правового обоснования и не отменяет обязанности доказывания.

То есть, мы видим, что предлагаемая модель предполагает проверку по четырём критериям: законное происхождение; сохранность и прослеживаемость информационного объекта; надлежащая процессуальная форма; фактическая проверяемость в условиях состязательности. И отрицательный ответ по одному из критериев не всегда механически означает одинаковое правовое последствие, характер дефекта должен оцениваться применительно к конкретным требованиям УПК РФ, а неустранённое нарушение, исключающее законное использование сведений, не может компенсироваться их визуальной убедительностью.

Практическим инструментом реализации модели может служить краткая учётная карточка цифрового материала, не заменяющая протоколы и постановления, в ней предлагается указывать идентификатор объекта, категорию и первоначальный источник, юридическое основание получения, дату, время и способ передачи, сведения об исходном и рабочем экземплярах, технические параметры сохранения, перечень выполненных преобразований, процессуальный документ, в котором материал исследован, а так же отметки о предоставленных возможностях проверки. Сведения же ограниченного доступа отражаются в установленном режиме. Законодательные же изменения представляются оправданными лишь

после оценки того, какие недостатки невозможно устранить на уровне надлежащего применения действующих норм. В частности, не следует вводить фикцию автоматической доказательственной силы цифровых записей или закреплять любой программный результат как самостоятельное доказательство, перспективнее нормативное уточнение требований к документированию электронного приложения и сохранению возможности его независимой проверки без нарушения конституционных гарантий.

В заключение можно сказать, что практическая реализация предложенного подхода возможна посредством совершенствования порядка представления цифровых приложений к результатам ОРД, разработки учётной карточки цифрового материала, организации согласованной работы с видеоархивами и повышения качества мотивировки процессуальных решений. Приоритет при этом должен принадлежать не количеству полученных записей, а законности, проверяемости и достаточности доказательственной информации при уважении прав участников массовых мероприятий.

Список литературы:

[1] Омелин В. Н. Актуальные проблемы представления результатов оперативно-розыскной деятельности органам предварительного расследования // Право и управление. 2026. № 8. С. 268–272.

[2] Омелин В. Н. К вопросу о понятии оперативно-розыскного обеспечения расследования преступлений // Право и управление. 2026. № 7. С. 325–328.

[3] Смушкин А. Б. Новые информационные компоненты в формировании электронных доказательств по уголовным делам (современная дорожка электронно-цифровых следов) // Сибирское юридическое обозрение. 2025. Т. 22. № 3. С. 455–468.

[4] Корнакова С. В., Чигрина Е. В. Электронные доказательства в российском уголовном процессе: проблемные вопросы // Юридический вестник Самарского университета. 2025. Т. 11. № 2. С. 44–50.

[5] Бугера М. А., Третьяков Ю. В. Применение видеозаписи как цифрового доказательства в современном уголовном процессе // Вестник Волгоградской академии МВД России. 2025. № 4. С. 120–126.

[6] Шайдаев М. Ш. Информационные технологии в охране общественного порядка и обеспечении общественной безопасности при проведении публичных и иных массовых мероприятий // Академическая мысль. 2024. № 2 (27).

[7] Петкевич Т. В. Применение современных технических средств дистанционного получения информации при проведении массовых мероприятий // Вестник Краснодарского университета МВД России. 2025. № 3 (69).

[8] Омелин В. Н. Законодательные ограничения проведения оперативно-розыскных мероприятий // Право и управление. 2026. № 1. С. 156–160.

[9] Зигура Н. А., Кудрявцева А. В. Компьютерная информация как вид доказательств в уголовном процессе России: монография. М.: Юрлитинформ, 2011. 176 с.

[10] Беппаев Р. Ж. Цифровой след как доказательство в уголовном процессе: проблемы допустимости и достоверности // Вопросы права. 2025. № 4. С. 51–54.

[11] Федеральный закон от 12 августа 1995 г. N 144-ФЗ "Об оперативно-розыскной деятельности". Текст Федерального закона опубликован в "Российской газете" от 18 августа 1995 г. N 160, в Собрании законодательства Российской Федерации от 14 августа 1995 г. N 33 ст. 3349.

[12] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. N 174-ФЗ. Текст Кодекса опубликован в "Российской газете" от 22 декабря 2001 г. N 249, в Собрании законодательства Российской Федерации от 24 декабря 2001 г. N 52 (часть I) ст. 4921, в "Парламентской газете" от 22 декабря 2001 г. N 241-242, от 25 декабря 2001 г. N 243-244, от 26 декабря 2001 г. N 245.

[13] Определение Конституционного Суда РФ от 4 февраля 1999 г. N 18-О "По жалобе граждан М.Б.Никольской и М.И.Сапронова на нарушение их конституционных прав отдельными положениями Федерального закона "Об оперативно-розыскной деятельности". Текст Определения опубликован в Вестнике Конституционного Суда Российской Федерации, 1999 г., N 3.

[14] Постановление Пленума Верховного Суда РФ от 29 ноября 2016 г. № 55 "О судебном приговоре". Текст постановления опубликован в "Российской газете" от 7 декабря 2016 г. N 277, в Бюллетене Верховного Суда Российской Федерации, январь 2017 г., N 1.

[15] Приказ МВД России, Министерства обороны РФ, ФСБ России, Федеральной службы охраны РФ, Федеральной таможенной службы, Службы внешней разведки РФ, Федеральной службы исполнения наказаний, Федеральной службы РФ по контролю за оборотом наркотиков, Следственного комитета РФ от 27 сентября 2013 г. N 776/703/509/507/1820/42/535/398/68 "Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд". Текст приказа опубликован в "Российской газете" от 13 декабря 2013 г. N 282.

References:

[1] Omelin V.N. Actual problems of presenting the results of operational-search activities to the preliminary investigation authorities // Law and management. 2026. № 8. PP. 268-272.

[2] Omelin V.N. To the question of the concept of operational-search support for the investigation of crimes // Law and management. 2026. № 7. S. 325-328.

[3] Smushkin A. B. New information components in the formation of electronic evidence in criminal cases (modern track of electronic-digital traces) // Siberian legal review. 2025. VOL. 22. № 3. S. 455-468.

[4] Kornakova S.V., Chigrina E.V. Electronic evidence in the Russian criminal process: problematic issues // Legal Bulletin of Samara University. 2025. T. 11. № 2. S. 44-50.

[5] Buguera M. A., Tretyakov Yu. V. The use of video recording as digital evidence in modern criminal proceedings // Bulletin of the Volgograd Academy of the Ministry of Internal Affairs of Russia. 2025. № 4. S. 120-126.

[6] Shaidaev M. Sh. Information technologies in the protection of public order and ensuring public safety during public and other mass events // Academic thought. 2024. № 2 (27).

[7] Petkevich T.V. The use of modern technical means of remote information acquisition during mass events // Bulletin of the Krasnodar University of the Ministry of Internal Affairs of Russia. 2025. № 3 (69).

[8] Omelin V.N. Legislative restrictions on the conduct of operational-search measures // Law and management. 2026. № 1. S. 156-160.

[9] Zigura N. A., Kudryavtseva A. V. Computer information as a type of evidence in the criminal process of Russia: monograph. M.: Yurlitinform, 2011. 176 s.

[10] R. Beppaev. Digital footprint as evidence in criminal proceedings: problems of admissibility and reliability // Legal issues. 2025. № 4. S. 51-54.

[11] Federal Law No. 144-FZ of August 12, 1995 "On Operational-Search Activities." The text of the Federal Law was published in Rossiyskaya Gazeta dated August 18, 1995 N 160, in the Collection of Legislation of the Russian Federation dated August 14, 1995 N 33 Art. 3349.

[12] Code of Criminal Procedure of the Russian Federation No. 174-FZ dated December 18, 2001. The text of the Code was published in Rossiyskaya Gazeta dated December 22, 2001 No. 249, in the Collection of Legislation of the Russian Federation dated December 24, 2001 No. 52 (part I) of Art. 4921, in Parlamentskaya Gazeta dated December 22, 2001 No. 241-242, dated December 25, 2001 No. 243-244, dated December 26, 2001 No. 245.

[13] Determination of the Constitutional Court of the Russian Federation of February 4, 1999 N 18-O "On the complaint of citizens M.B. Nikolskaya and M.I. Sapronov about violation of their constitutional rights by certain provisions of the Federal Law "On Operational-Search Activities." The text of the Decision is published in the Bulletin of the Constitutional Court of the Russian Federation, 1999, No. 3.

[14] Resolution of the Plenum of the Supreme Court of the Russian Federation of November 29, 2016 No. 55 "On the court verdict." The text of the decision was published in Rossiyskaya Gazeta dated December 7, 2016 No. 277, in the Bulletin of the Supreme Court of the Russian Federation, January 2017, No. 1.

[15] Order of the Ministry of Internal Affairs of Russia, the Ministry of Defense of the Russian Federation, the Federal Security Service of the Russian Federation, the Federal Customs Service, the Foreign Intelligence Service of the Russian Federation, the Federal Penitentiary Service, the Federal Drug Control Service of the Russian Federation, of September 27, 2013 N 776/703/509/507/1820/42/535/398/68 "On approval Instructions on the procedure for submitting the results of operational-search activities to the inquiry body, investigator or court." The text of the order was published in Rossiyskaya Gazeta dated December 13, 2013 No. 282.