

Научная статья

УДК 340.1

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ СИСТЕМЫ «БЕЗОПАСНЫЙ ГОРОД» В ПРОЦЕССЕ ДОКАЗЫВАНИЯ ПО УГОЛОВНЫМ ДЕЛАМ

Антон Антонович АНТОНОВ

Университета Прокуратуры Российской Федерации, Санкт-Петербург, Россия
Antonovantonag2@gmail.com

Давид Сергеевич ГУДКОВ

Университета Прокуратуры Российской Федерации, Санкт-Петербург, Россия
Goodkooov545@gmail.com

Екатерина Андреевна ПРОТАСОВА

Университета Прокуратуры Российской Федерации, Санкт-Петербург, Россия
Protasovaalla9@gmail.com

Научный руководитель доцент кафедры уголовного процесса и криминалистики Санкт-Петербургского юридического института (филиала) Университета Прокуратуры Российской Федерации, кандидат юридических наук, доцент, советник юстиции **Елена Владимировна БАРКАЛОВА**
elena_vallask@mail.ru

Аннотация. В статье рассматривается использование системы «Безопасный город» в уголовном процессе. Авторами предпринята попытка продемонстрировать возможности использования результатов применения указанной системы в качестве доказательств по уголовному делу с соблюдением определенного порядка получения такой информации. Раскрываются правовые основания включения цифровых сведений в систему доказательств с опорой на нормы процессуального законодательства. Особое внимание уделено практическим рискам: ограниченный срок хранения видеоматериалов, возможность утраты данных и иные. В работе обосновывается детализация процессуальных требований к электронным доказательствам: фиксация идентификатора источника, временные метки, способы копирования. Отдельное внимание уделено обеспечению

состязательности в уголовном процессе - _ _гарантиям доступа стороне защиты к исходным данным, лежащим в основе автоматизированных выводов.

Ключевые слова: криминалистика, уголовный процесс, система «Безопасный год», электронные доказательства, цифровые данные, видеонаблюдение, искусственный интеллект.

SPECIFIC FEATURES OF USING THE "SAFE CITY" SYSTEM IN CRIMINAL CASE EVIDENCE PROCEEDINGS

Anton Antonovich ANTONOV

University of the Prosecutor's Office of the Russian Federation, St. Petersburg, Russia

Antonovantonag2@gmail.com

David Sergeevich GUDKOV

University of the Prosecutor's Office of the Russian Federation, St. Petersburg, Russia

Goodkooov545@gmail.com

Ekaterina Andreevna PROTASOVA

University of the Prosecutor's Office of the Russian Federation, St. Petersburg, Russia

Protasovaalla9@gmail.com

Scientific Supervisor: Associate Professor of the Department of Criminal Procedure and Forensic Science of the St. Petersburg Law Institute (branch) of the University of the Prosecutor's Office of the Russian Federation, Candidate of Legal Sciences, Associate Professor, Advisor of **Justice Elena Vladimirovna BARKALOVA**

Annotation. The article examines the use of the “Safe City” system in criminal proceedings. The authors attempt to demonstrate the possibilities of using the results of applying this system as evidence in a criminal case, subject to a certain procedure for obtaining such information. The legal grounds for including digital information in the system of evidence are disclosed, relying on the norms of

procedural legislation. Special attention is paid to practical risks: the limited storage period for video materials, the possibility of data loss, and others. The paper substantiates the detailed specification of procedural requirements for electronic evidence: фиксация идентификатора источника, временные метки, methods of copying. Special attention is paid to ensuring adversarial proceedings in criminal proceedings — to guarantees of the defense party's access to the original data underlying automated conclusions.

Keywords: criminology, criminal procedure, the “Safe Year” system, electronic evidence, digital data, video surveillance, artificial intelligence.

В настоящее время цифровизация влияет на все сферы жизни человека. Во многом именно в результате цифровизации жизнь человека становится более организованной, в связи с этим, актуализируется вопрос внедрения новых технологий и в деятельность следственных органов. Так, например, были созданы автоматизированные информационно-поисковые системы «Картотека», «Розыск номерных вещей», «Сейф», «Розыск оружия», а также автоматизированная дактилоскопическую идентификационная система «Папилон».

В последние годы наблюдается также активное внедрение аппаратно-программного комплекса «Безопасный город», интегрирующего видеонаблюдение, мониторинговые датчики, системы отслеживания динамических объектов и аналитические модули. Согласно Распоряжению Правительства РФ от 3 декабря 2014г. №2446-р¹, перед комплексом ставится задача построения и развития единого системного подхода к обеспечению общественной безопасности и правопорядка.

На практике уже заметна востребованность данной инфраструктуры. В Санкт-Петербурге в 2025 году, по заявлению вице-губернатора города,

¹ Распоряжение Правительства РФ от 03.12.2014 № 2446-р «Об утверждении Концепции построения и развития аппаратно-программного комплекса "Безопасный город"» // Собрание законодательства РФ. 2014. № 50. Ст. 7188.

полицейские раскрыли с её помощью более 1900 преступлений; также приводилась динамика раскрываемости угонов с 6 процентов до почти 50 процентов². В Москве в 2025 году, по данным, которые озвучили представители правоохранительных органов, с помощью камер было раскрыто около двух тысяч преступлений, а за десять лет число квартирных краж сократилось в 34,5 раза³. В Калининградской области по итогам 2025 года с помощью технических средств АПК «Безопасный город» раскрыто 101 преступление и выявлено 484 административных правонарушения без учета нарушений ПДД⁴. Это позволяет сделать вывод, что городская цифровая инфраструктура все чаще выступает источником сведений, которые имеют непосредственное значение для установления обстоятельств уголовного дела.

Отдельного внимания заслуживает вопрос о том, какое место в системе доказательств будут занимать такие сведения. С.В. Корнакова и Е.В. Чигрина, анализируя ч. 2 ст. 74 УПК РФ, отмечают, что «...электронные носители информации пока не выделяются законодателем в самостоятельную разновидность доказательств как «электронные доказательства». Именно это обстоятельство может послужить поводом к дискуссии о необходимости внесения соответствующих изменений в Уголовно-процессуальный кодекс Российской Федерации, поскольку закон не содержит достаточно четких требований к понятию и способам удостоверения компьютерной

² О состоянии правопорядка и результатах работы систем видеонаблюдения АПК «Безопасный город» в Санкт-Петербурге: Отчет Комитета по информатизации и связи Санкт-Петербурга [Электронный ресурс]. URL: <https://kis.gov.spb.ru/docs/> (дата обращения: 19.09.2026).

³ Отчет Главного управления МВД России по г. Москве о результатах оперативно-служебной деятельности и эффективности использования системы видеонаблюдения [Электронный ресурс]. URL: https://77.мвд.рф/dlya_grajdan/отчеты (дата обращения: 19.09.2026).

⁴ Отчет об итогах деятельности Государственного казенного учреждения Калининградской области «Безопасный город» [Электронный ресурс]. URL: <https://svyaz.gov39.ru/activity/connection/city/> (дата обращения: 19.09.2026).

информации⁵, а развитие технологий опережает обновление нормативной базы»⁶.

В данном случае значение будет иметь конкретная форма получения информации и то, каким процессуальным документом подтверждено ее происхождение. Согласно статье 74 УПК РФ, доказательствами признаются любые сведения, на основе которых суд, прокурор, следователь и дознаватель устанавливают обстоятельства, подлежащие доказыванию при производстве по уголовному делу⁷. Частью 2 статьи 84 УПК РФ прямо допускается в качестве доказательств использовать фото- и киносъемку, аудио- и видеозаписи и иные носители информации. Соответственно цифровые данные «Умного города» могут быть включены в существующую систему доказательств.

Согласно ст. 85 УПК РФ доказывание включает собирание, проверку и оценку доказательств, а ст. 86 УПК РФ связывает их собирание с производством предусмотренных Уголовно-процессуальным кодексом РФ следственных и иных процессуальных действий. Существенное значение в рассматриваемом контексте имеет и ст. 21 УПК РФ, предусматривающая обязанность органов предварительного расследования принимать меры к установлению события преступления и лиц, его совершивших, а в части 4 указанной статьи зафиксирована норма, согласно которой требования, поручения и запросы, предъявленные в пределах полномочий, обязательны для исполнения организациями и должностными лицами. Следовательно,

⁵ Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 12.12.2025) «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 19.09.2026).

⁶ 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. С. 45.

⁷ Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 26.07.2026) [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 19.09.2026)

оператор городской системы, у которого находятся нужные сведения, должен рассматриваться прежде всего как источник информации, к которому применяется соответствующий процессуальный механизм получения данных.

В этой связи следует учитывать не только момент направления запроса оператору, но и то, какая именно запись должна быть сохранена. Желательно истребовать исходный фрагмент без самостоятельной «обрезки» со стороны следователя, а также сведения о времени начала и окончания записи, номере камеры, техническом адресе оборудования и факте последующего экспорта. Такой порядок позволяет отделить первичную информацию от ее копии и в дальнейшем ответить на вопрос, не изменился ли материал при выгрузке.

Что необходимо сделать на стадии проведения проверки сообщения о преступлении? Так, например, статья 144 УПК РФ позволяет истребовать документы и предметы, проводить их осмотр, привлекать специалистов, а полученные сведения использовать в качестве доказательств при соблюдении требований ст. 75 и 89 УПК РФ. Для систем «Безопасного города» это имеет практическое значение из-за ограниченных сроков хранения видео и журналов событий. Сведения, которые не были своевременно сохранены, могут быть автоматически перезаписаны, поэтому при расследовании преступления требуется вовремя определить требуемый временной интервал и направить оператору требование о сохранении соответствующего массива с указанием камеры, времени, участка территории и других идентификаторов. Такой подход позволяет предотвратить утрату исходных данных еще до проведения основных следственных действий.

Практика Верховного Суда Российской Федерации свидетельствует о том, что проблема срока хранения видеозаписей имеет не теоретический, а вполне прикладной характер. Так, кассационным определением Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 2

июля 2024 г. № 66-УДП24-9сп-А5 было установлено, что в архиве суда записи с камер видеонаблюдения хранились 12 дней, вследствие чего к моменту обращения потерпевшей соответствующий материал уже был удален. Сам по себе этот факт не был признан достаточным для удовлетворения жалобы, однако приведенный пример наглядно показывает негативные последствия несвоевременного обращения за предоставлением цифровой информации⁸.

Кроме того, не менее важен способ фиксации цифрового материала. Так, часть 6 статьи 164 УПК РФ допускает применение технических средств при обнаружении, фиксации и изъятии следов преступления, в свою очередь, ч. 5 ст. 166 УПК РФ предусмотрено требование об отражении в протоколе следственного действия примененных технических средств, условий и порядка их использования, объектов воздействия и полученных результатов. К протоколу могут прилагаться электронные носители информации, полученной или скопированной в ходе следственного действия. Следовательно, при работе с городской информационной системой следует описывать не только содержание видео, но и процедуру выгрузки: наименование системы, идентификатор камеры, дату и время, используемое программное обеспечение, формат файла, способ копирования, вид носителя и сведения о лице, осуществившем экспорт. Чем подробнее зафиксирована процедура получения, тем выше возможность проверить происхождение данных, а значит меньше вероятность оспорить их достоверность.

Современные системы способны распознавать государственные регистрационные знаки, отслеживать перемещение объектов, выявлять

⁸ Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 02.07.2024 № 66-УДП24-9сп-А5 [Электронный ресурс]. URL: <https://legalacts.ru/sud/kassatsionnoe-opredelenie-sudebnoi-kollegii-po-ugolovnym-delam-verkhovnogo-suda-rossiiskoi-federatsii-ot-03072024-n-66-udp24-9sp-a5/> (дата обращения: 19.09.2026).

нахождение человека в определенной зоне, а также наделены функцией распознавания лица. Однако алгоритмический результат нельзя приравнивать к факту, поскольку сообщение программы о совпадении является результатом обработки первичных данных, а не наблюдением действительности, поэтому сведения, сформированные искусственным интеллектом, следует использовать как основание для поиска и проверки, а выводы строить на совокупности исходных кадров, метаданных, показаний и иных доказательств. В противном случае, возникает риск фактической замены процесса доказывания выводами нейросети. Автоматизированный поиск по камерам, транспортным потокам и иным объектам городской инфраструктуры может использоваться как средство обнаружения нужного фрагмента, однако результаты такой фильтрации не должны смешиваться с исходной информацией. Иначе сложится ситуация, при которой следствие фактически оценивает не сам цифровой след, а уже интерпретированный программой результат.

В пункте 16 Постановления Пленума Верховного Суда РФ «О практике применения законодательства при рассмотрении уголовных дел в суде первой инстанции (общий порядок судопроизводства)» от 19 декабря 2017 г. № 51 указано, что специалист может привлекаться для оказания содействия сторонам и суду в осмотре предметов и документов, применении технических средств и разъяснении вопросов, входящих в его профессиональную компетенцию, а в пункте 17 прямо предусмотрена возможность допроса в рамках судебного заседания об обстоятельствах производства следственного

действия по вопросам, входящим в его профессиональную компетенцию, а также разъяснения выраженного им суждения по этим вопросам⁹.

Так, специалист необходим, когда следователю требуется помощь в копировании данных, описании архитектуры системы, толковании журналов событий или установлении технических параметров. Экспертное исследование востребовано там, где необходимо решить специальные вопросы, например, установить факт изменения файла, исследовать признаки монтажа, восстановить информацию, проверить правильность функционирования конкретного программно-технического комплекса. При этом окончательная оценка результата должна оставаться предметом доказывания и осуществляться с учетом принципов относимости, допустимости, достоверности и достаточности доказательств (часть 1 статьи 88 УПК).

М. И. Воронин отмечает, что «цифровая информация в исходной форме не воспринимается человеком непосредственно и требует преобразования с помощью технических средств, вследствие чего при работе с ней важное значение приобретает не только содержание файла, но и способ его формирования и воспроизведения»¹⁰. Для системы «Безопасный город» это особенно заметно, поскольку один и тот же материал может существовать в виде исходного потока, архивного файла, выгрузки оператора и уже обработанного следователем фрагмента. Каждая такая операция может иметь значение при дальнейшей проверке доказательства.

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» в ст. 5 устанавливает принципы законности, определенности целей и

⁹ Постановление Пленума Верховного Суда РФ от 19.12.2017 № 51 (ред. от 09.12.2025) «О практике применения законодательства при рассмотрении уголовных дел в суде первой инстанции (общий порядок судопроизводства)», пп. 16–17 // Российская газета. 2017. № 292.

¹⁰ Воронин М. И. О правовой природе электронных (цифровых) доказательств // Lex russica. 2020. № 10 (74). С. 75–76.

недопустимости избыточной обработки, а ст. 7 закрепляет обязанность соблюдать конфиденциальность персональных данных¹¹. Особое значение имеет статья 11 указанного закона, регламентирующая биометрические персональные данные, такие как параметры лица. В данной статье предусмотрены специальные правила обработки сведений, используемых для установления личности, и прямо названы случаи, когда такая обработка допускается без согласия субъекта, в том числе в связи с осуществлением правосудия и в предусмотренных законодательством случаях в сфере безопасности, оперативно-розыскной и уголовно-процессуальной деятельности. В связи с этим при использовании распознавания лиц и камер системы «Безопасный город» необходимо различать обычную видеозапись, обработку изображения и собственно автоматизированную биометрическую идентификацию.

В работе А.С. Бондарева, А.П. Нагорного и А.С. Чупрова сделан акцент на том, что электронные доказательства отличаются от традиционных в том числе зависимостью от технических средств, программного обеспечения и условий воспроизведения. В частности, цифровая информация, по мнению авторов, может быть изменена без очевидных внешних следов, а ее восприятие человеком возможно только после преобразования с помощью соответствующих устройств и программ.¹² Существенное значение имеет в том числе и сохранение процессуального порядка обращения с цифровыми данными, поскольку нарушение порядка обнаружения, изъятия, копирования или хранения способно поставить под сомнение их доказательственное значение. Применительно к городским системам это подтверждает то, что

¹¹ Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 26.07.2026) «О персональных данных» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 19.09.2026).

¹² Бондарев А. С., Нагорный А. П., Чупров А. С. Электронные доказательства в уголовном процессе на современном этапе // Вестник Краснодарского университета МВД России. 2021. № 2 (52). С. 137–139.

желательно фиксировать не только содержание видеозаписи, но и весь её путь от получения от информационной системы до приобщения к материалам дела.

Кроме того, стоит разграничивать в материалах дела первичные данные, результаты обработки и процессуальные выводы. Первичный уровень включает исходную видеозапись, временные метки, технические журналы и сведения о состоянии оборудования. Второй уровень образуют распознанные номера, отчеты видеоаналитики и построенные системой маршруты. Третий уровень - это протоколы осмотра, заключения специалиста или эксперта и показания лиц, объясняющих порядок формирования данных. Доказательственный вывод должен по возможности опираться на связь всех трех уровней, а не только на нейросетевой отчет.

Обращаем внимание на то, что информационная инфраструктура охраняется вышеупомянутым Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»¹³ регулирующим вопросы связанные с информационными технологиями, информацией, её защитой, а также передачей, обработкой и использованием данных посредством компьютерных систем и сетей. Так, в статье 16 ФЗ № 149-ФЗ закрепляются правовые, организационные и технические меры защиты информации от неправомерного доступа, уничтожения и модификации.

В качестве общего процессуального алгоритма можно предложить следующую последовательность, изложенную без привязки к конкретному типу городской системы: сначала определить, какие данные нужны для проверки версии и в каком временном диапазоне они существуют; затем

¹³ Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 12.12.2025) «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 19.09.2026).

незамедлительно обеспечить сохранность исходного массива; после этого получить копию предусмотренным законом способом с фиксацией технических условий, провести осмотр и при необходимости привлечь специалиста; далее сопоставить данные с другими доказательствами и только после этого дать им оценку согласно ст. 88 УПК РФ. Такая последовательность позволяет соединить технологическую специфику «Безопасного города» с общими гарантиями прав и законных интересов участников уголовного процесса.

Целесообразно также предусмотреть требования в УПК РФ к указанию идентификатора источника, времени создания данных, способа получения и копирования, сведений о программных преобразованиях и контроля целостности. На уровне ведомственных регламентов следует установить сроки срочного сохранения информации, порядок формирования выгрузок, правила ведения журналов доступа и обязанность предоставлять исходные файлы по процессуальному запросу. Отдельно необходимо обеспечить состязательность при использовании алгоритмов: сторона защиты должна иметь реальную возможность исследовать не только итоговый вывод системы, но и исходные данные, ставшие его основой.

Таким образом, система «Умный город» становится значимым элементом доказательственной среды уголовного судопроизводства. Ее особенности состоят в массовом характере данных, автоматизированной обработке, зависимости от технического состояния инфраструктуры и необходимости одновременно соблюдать требования УПК РФ и законодательства о защите информации. Действующий уголовно-процессуальный закон уже позволяет использовать такие сведения через документы, вещественные доказательства, протоколы и экспертные исследования, однако развитие цифровой инфраструктуры требует большей

детализации правил их получения и проверки. Основным условием надежности должно быть сохранение происхождения данных, их целостности и возможности для суда и сторон проверить способ формирования и обоснованность автоматизированных выводов.

Список источников

Нормативные правовые акты и судебная практика:

1. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 26.07.2026) [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 17.09.2026).
2. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 12.12.2025) «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 19.09.2026).
3. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 08.08.2024) «О персональных данных» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 19.09.2026).
4. Распоряжение Правительства Российской Федерации от 03.12.2014 № 2446-р «Об утверждении Концепции построения и развития аппаратно-программного комплекса "Безопасный город"» // Собрание законодательства РФ. 2014. № 50. Ст. 7188.
5. Постановление Пленума Верховного Суда Российской Федерации от 19.12.2017 № 51 (ред. от 09.12.2025) «О практике применения законодательства при рассмотрении уголовных дел в суде первой инстанции (общий порядок судопроизводства)» // Российская газета. 2017. № 292.

6. Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 02.07.2024 № 66-УДП24-9сп-А5 [Электронный ресурс]. URL: <https://legalacts.ru/sud/kassatsionnoe-opredelenie-sudebnoi-kollegii-po-ugolovnym-delam-verkhovnogo-suda-rossiiskoi-federatsii-ot-03072024-n-66-udp24-9sp-a5/> (дата обращения: 19.09.2026).

Научная литература:

1. Бондарев А. С., Нагорный А. П., Чупров А. С. Электронные доказательства в уголовном процессе на современном этапе / А. С. Бондарев, А. П. Нагорный, А. С. Чупров // Вестник Краснодарского университета МВД России. – 2021. – № 2 (52). С. 137–141.
2. Воронин М. И. О правовой природе электронных (цифровых) доказательств / М. И. Воронин // Lex russica. – 2020. – № 10 (74). С. 74–81.
3. Корнакова С. В., Чигрина Е. В. Электронные доказательства в российском уголовном процессе: проблемные вопросы / С. В. Корнакова, Е. В. Чигрина // Юридический вестник Самарского университета. – 2025. – Т. 11, № 2. С. 44–50.