Научная статья
https://doi.org/:10.29039/2312-7937-2026-1-82-87
EDN: https://elibrary.ru/fgqisf

ИСАЕВА ЕЛЕНА ДМИТРИЕВНА
кандидат юридических наук
Брянский филиал ОрЮИ МВД России
им. В. В. Лукьянова
(Брянск, Россия)
isaevaelena190373@yandex.ru

ЗАШАКУЕВ АЗАМАТ ЗАУРОВИЧ
Северо-Кавказский институт повышения квалификации (филиал)
Краснодарского университета МВД России
(Нальчик, Россия)
a.zashakuyev@mail.ru

АЛГОРИТМ ПЕРВОНАЧАЛЬНЫХ ДЕЙСТВИЙ СОТРУДНИКОВ ПОЛИЦИИ ПО ПРИБЫТИИ НА МЕСТО ПРЕСТУПЛЕНИЯ, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. *В условиях цифровой трансформации общества и роста киберпреступности первоначальные действия сотрудников полиции на месте преступления приобретают критическое значение. Преступления с использованием информационно-коммуникационных технологий (ИКТ) отличаются от традиционных преступлений спецификой объекта, следов, доказательств и технологическими особенностями. От своевременности, корректности и законности действий первых реагирующих подразделений – патрульно-постовой службы полиции, дежурных частей, оперативных групп – зависит не только раскрытие преступления, но и допустимость доказательств в суде.*

В статье анализируются правовые основы, тактические схемы, организационные и технологические аспекты первоначальных действий сотрудников полиции при выезде на место преступления с применением информационно-коммуникационных технологий. На основе анализа судебной практики, нормативных актов предложена модель первоначальных действий, адаптированных под специфику цифровых следов. Особое внимание уделено вопросам сохранения цифровых следов, изъятия электронных носителей, взаимодействия с экспертами и правилам документирования.

Ключевые слова: *киберпреступление, информационно-коммуникационные технологии, первоначальные действия, место преступления, криминалистика, цифровые доказательства, изъятие электронных носителей, полиция, следственный эксперимент, законность доказательств*

Для цитирования: *Исаева Е. Д., Зашакуев А. З. Алгоритм первоначальных действий сотрудников полиции по прибытии на место преступления, совершенного с использованием информационно-коммуникационных технологий // Вестник ВИПК МВД России. 2026. № 1 (77). С. 82–87; https://doi.org/:10.29039/2312-7937-2026-1-82-87.*

ISAEVA ELENA D.
phd of law
Bryansk Branch of Lukianov Orel law institute of the Ministry of the Interior of Russia
(Bryansk, Russia)

ZASHAKUEV AZAMAT Z.
North Caucasus Advanced Training Institute (branch)
Krasnodar University of the Ministry of Internal Affairs of Russia
(Nalchik, Russia)

ALGORITHM OF THE FIRST ACTIONS TAKEN BY POLICE OFFICERS ON ARRIVAL AT A CRIME SITE COMMITTED USING INFORMATION AND COMMUNICATION TECHNOLOGIES

Abstract. *In the context of the digital transformation of society and the growth of cybercrime, the initial actions of police officers at the crime scene are of critical importance. Crimes involving information and communication technologies (ICTs) differ from traditional crimes in terms of the specific nature of the object, traces, evidence, and technological features. The timely, correct, and legal actions of the first responding units, such as the police patrol service, duty stations, and operational groups, not only determine the success of the crime investigation, but also the admissibility of evidence in court.*

The article analyzes the legal basis, tactical schemes, organizational and technological aspects of the initial actions of police officers when they arrive at a crime scene using information and communication technologies. Based on the analysis of judicial practice and regulatory acts, a model of initial actions adapted to the specifics of digital traces is proposed. Special attention is paid to the issues of preserving digital traces, removing electronic media, interacting with experts, and the rules of documentation.

Keywords: *cybercrime, information and communication technologies, initial actions, crime scene, forensics, digital evidence, seizure of electronic media, police, investigative experiment, legality of evidence*

For citation: *Isaeva E. D., Zashakuev A. Z. Algorithm of the first actions taken by police officers on arrival at a crime site committed using information and communication technologies // Vestnik Advanced Training Institute of the MIA of Russia. 2026. № 1 (77). P. 82–87; https://doi.org/:10.29039/2312-7937-2026-1-82-87.*

Современное общество находится на этапе глубокой цифровой трансформации. По данным Росстата, на 2025 год более 98 % населения России в возрасте 15–74 лет имеют доступ к интернету, а 87 % регулярно используют онлайн-сервисы для оплаты, общения, работы и управления финансами. Этот процесс, с одной стороны, способствует повышению качества жизни, с другой – создаёт беспрецедентные возможности для преступных действий.

Согласно данным МВД России за 2025 год, количество выявленных преступлений с использованием информационно-коммуникационных технологий (далее – ИКТ) достигло 312 800 случаев, что на 22 % выше показателя 2024 года. При этом более 65 % из них – это преступления, совершаемые вне физического места традиционного преступления (например, хакерские атаки, фишинг, криптовалютные скамы), сопровождающиеся физическим следствием: взломом офиса, похищением компьютера, утечкой данных из локальной сети, использованием устройств в доме жертвы и т. п.[1]

Место совершения преступлений с использованием информационно-коммуникационных технологий или киберпреступлений имеет двойственную природу – это не только физическое пространство, но и цифровая среда, в которой могут находиться ключевые доказательства: смартфоны, ноутбуки, роутеры, облачные хранилища, журналы доступа, IoT-устройства, умные часы, системы видеонаблюдения и даже умные холодильники с записью голоса.

Первые реагирующие сотрудники подразделений полиции – патрульно-постовой службы, дежурных частей, оперативных групп – зачастую не обладают достаточной подготовкой для работы с такими объектами. Включение выключенных устройств приводит к уничтожению временных файлов, попытка «проверить» телефон – к удалению сообщений, уничтожению данных из облачных сервисов, отсутствию фиксации адресов роутеров, что делает невозможным восстановление логов, и наконец, неправильное составление протоколов осмотра места происшествия ведет к признанию доказательств недопустимыми.

Анализ судебной практики показывает, что в 2024–2025 гг. более 43 % уголовных дел о киберпреступлениях были прекраще-

[1] Государственный статистический отчет ФКУ «ГИАЦ МВД России». URL: http.mvd.ru (дата обращения: 12.01.2026).

ны или признаны необоснованными именно из-за нарушений при первоначальных действиях на месте происшествия[1].

Таким образом, актуальность темы обусловлена ростом числа преступлений с использованием информационно-коммуникационных технологий, спецификой цифровых следов, требующих иного подхода к их сбору и сохранению, и риском признания доказательств недопустимыми в суде.

Согласно ст. 74 Уголовно-процессуального кодекса РФ (далее – УПК РФ), доказательства – это сведения, на основе которых устанавливается наличие или отсутствие обстоятельств, подлежащих доказыванию. Главное требование к этим сведениям – они должны быть получены и закреплены в строгом соответствии с процедурами, определенными УПК РФ (принцип допустимости доказательств). Доказательства, полученные с нарушением требований УПК РФ, признаются недопустимыми и не могут использоваться для обоснования обвинения или принятия судебного решения.

Цифровые доказательства, будучи хрупкими и легко изменяемыми, требуют специальных процедур для обеспечения их допустимости и достоверности. Чтобы сведения, полученные из цифровых источников, могли стать законными доказательствами в суде, соответствовать ст. 74 УПК РФ и принципу допустимости, необходимо строгое соблюдение процессуальных норм. Сбор, извлечение и фиксация данных должны проводиться в рамках следственных действий, предусмотренных УПК РФ, с обязательным участием специалистов и понятых.

Международные стандарты по идентификации, сбору, получению и хранению цифровых свидетельств (доказательств), ISO/IEC 27037:2012, NIST SP 800-86 предлагают единые подходы к идентификации, сбору, получению и хранению цифровых свидетельств (доказательств).

ISO/IEC 27037:2012 – международный стандарт, имеющий аутентичный российский национальный стандарт ГОСТ Р ИСО/МЭК 27037-2014[2], определяющий руководство по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме.

NIST SP 800-86 – специальная публикация Национального института стандартов и технологий США (NIST) под названием «Руководство по интеграции методов криминалистики в реагирования на инциденты»[3], не имеет прямого официального российского аналога в виде национального стандарта (ГОСТ Р), который бы полностью дублировал его содержание. Тем не менее принципы и рекомендации, изложенные в этом американском руководстве, активно используются российскими специалистами и находят отражение в ряде российских нормативных документов и практик.

Стандарты имеют разные акценты. ГОСТ Р ИСО/МЭК 27037-2014 более детально фокусируется на технических процедурах и конкретных действиях, которые должен предпринять «первый респондент» при работе с различными типами носителей (мобильные, сетевые, облачные). Это пошаговое руководство по правильному обращению с уликами. NIST SP 800-86 фокусируется больше на управленческом подходе и интеграции методов криминалистики в общие организационные процессы реагирования на инциденты информационной безопасности и предназначен для ИТ-служб компаний.

Оба вида стандарта являются взаимодополняющими, а не взаимоисключающими и используются совместно для создания комплексной и юридически обоснованной процедуры работы с цифровыми доказательствами, однако их внедрение в российскую практику сталкивается с правовыми, техническими и организационными барьерами.

Алгоритм первоначальных действий сотрудников полиции по прибытии на место преступления, совершенного с использованием ИКТ, направлен на обеспечение сохранности цифровых доказательств до приезда квалифицированных сотрудников и экспертов.

Так, Российский национальный стандарт ГОСТ Р ИСО/МЭК 27037-2014 имеет название «Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме».

[1] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 (дата обращения: 12.01.2026).

[2] Национальный стандарт Российской Федерации. URL: https://ohranatruda.ru/upload/iblock/d30/4293768989.pdf (дата обращения: 12.01.2026).

[3] Руководство по интеграции методов криминалистики в реагирования на инциденты. URL: https://csrc.nist.gov/pubs/sp/800/86/final (дата обращения: 12.01.2026).

ГОСТ служит подробным методическим руководством для сотрудников полиции, первыми прибывающих на место происшествия, где могут находиться цифровые доказательства. Ключевой целью стандарта выступает обеспечение сохранения целостности и подлинности цифровых данных, что критически важно для их юридической допустимости в качестве доказательств в суде.

Стандарт ИСО/МЭК 27037-2014 фокусируется на четырех основных взаимосвязанных процессах: идентификация, сбор, получение, хранение. Говоря об алгоритме первоначальных действий сотрудников полиции по прибытии на место преступления, совершенного с использованием ИКТ, до приезда квалифицированных сотрудников или экспертов, предлагается разобрать два процесса рассматриваемого ГОСТа – идентификация и сбор.

Прибытие на место преступления, совершенного с использованием ИКТ, требует от сотрудников особых неотложных действий, направленных на сохранение цифровых доказательств, которые являются крайне хрупкими. Опираясь на ст. 12 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции», в дополнение к стандартным обязанностям сотрудники должны выполнить специфические задачи по документированию обстоятельств преступления и обеспечению сохранности следов.

Процесс идентификации цифровых доказательств – это определение того, какие объекты на месте преступления могут содержать цифровую информацию, имеющую отношение к делу. Главный принцип идентификации – «минимальное вмешательство – максимальная фиксация».

По прибытии на место происшествия необходим визуальный осмотр с целью выявления электронных устройств (которые могут входить в перечень цифровых объектов), находящихся на месте совершения преступления. К ним относятся: включённые компьютеры, ноутбуки, смартфоны, подключённые USB-накопители, внешние диски, Wi-Fi роутеры, умные колонки, камеры, наушники, микрофоны, динамики. Любые электронные устройства могут содержать логи доступа – автоматически создаваемые записи, как правило в виде текстовых файлов, о всех событиях, связанных с попытками доступа к определенной системе, ресурсу, файлу или сетевому сервису.

Для предотвращения удаления или изменения данных, которые впоследствии могут послужить цифровыми доказательствами, необходимо придерживаться трех основных принципов:

1. *Принцип целостности* – исключение любого изменения цифровых данных с момента их обнаружения.

Цифровое доказательство – это любая информация, представленная в цифровой форме, которая может быть использована для установления обстоятельств преступления: данные с компьютеров и серверов, мобильные устройства (смартфоны, планшеты), облачные хранилища (Google Drive, Яндекс.Диск, iCloud), журналы доступа, логи сетевых устройств, данные IoT-устройств (умные камеры, носимые гаджеты), электронная переписка, посты в социальных сетях, криптовалютные транзакции.

Специфика цифровых доказательств выражается в отсутствии физической формы, возможности создания и удаления за секунды, содержании миллионов записей в одном файле, легкости редактирования без следов.

Задача сотрудников полиции, первыми прибывших на место совершения преступления с использованием ИКТ, – «заморозить» ситуацию и предотвратить изменения, для чего необходимо минимизировать любое физическое взаимодействие с электронными устройствами.

Существует критическое правило: если устройство включено – оставлять включённым, если выключено – не включать. Выключение приводит к потере энергозависимых данных (оперативная память, активные соединения), что необратимо нарушает целостность улик. Попытки самостоятельно просмотреть или попробовать разблокировать электронное устройство загрязняют улики собственными действиями сотрудника, изменяют данные и ставят под сомнение объективность доказательств.

2. *Принцип документирования* – фиксация всех действий с электронными носителями информации. Все действия и состояние оборудования должны фиксироваться на видео [1, с. 58–61].

В рапорте об обнаружении признаков преступления необходимо отразить обстоятельства своего прибытия и принятые меры (оказание помощи, задержание, оцепление) [2, с. 71–72]. В случае «цифрового» преступления рапорт дополняется перечнем обнаруженных электронных устройств, в том числе описанию подлежат:

• Перечень обнаруженных электронных устройств, который помогает в дальнейшем следствию точно знать, какие объекты были на месте и какие из них потенциально содержат доказательства. Точное описание каждого объекта позволяет отследить его перемещение с момента обнаружения до помещения на хранение или передачи эксперту.

• Состояние устройств (включены/выключены) – сигнал для прибывающего специалиста, что на носителе, вероятно, присутствует энергозависимая информация (данные в оперативной памяти), которую необходимо извлекать определенным образом, прежде чем физически обесточить устройство. Кроме того, это также важная информация, гарантирующая, что первоначальное состояние системы зафиксировано и не было изменено сотрудниками полиции.

• Опрос потерпевших и очевидцев о том, кто пользовался устройствами, когда и что именно произошло.

Это требование напрямую связано с необходимостью соблюдения принципа целостности цифровых доказательств, о котором говорилось ранее, и обеспечения их допустимости согласно ст. 74 УПК РФ.

Неприменение или неправильное использование персональных видеорегистраторов, отсутствие детальных фотографий и описаний обстановки до вмешательства, поверхностное описание в рапорте или протоколе состояния оборудования, расположения кабелей и содержания экранов мониторов напрямую влияет на эффективность всего дальнейшего расследования и возможность использования собранных сведений в качестве легитимных доказательств в суде.

Одной из ключевых задач сотрудников полиции, первыми прибывающих на место преступления с использованием ИКТ, является обеспечение сохранности цифровых доказательств до прибытия специалистов-криминалистов. Непрофессиональные действия могут привести к безвозвратной утрате критически важной информации.

Процесс сбора цифровых доказательств в контексте действий сотрудников полиции, первыми пребывающих на место происшествия, означает физическое изъятие носителей и обеспечение их сохранности (хранение), а не извлечение данных.

3. *Принцип минимального вмешательства* – ограничение взаимодействия с потенциальными источниками доказательств. Этот принцип вытекает из необходимости соблюдения целостности цифровых доказательств и является фундаментальным для обеспечения допустимости доказательств в уголовном процессе.

Реализуется посредством установления физического периметра вокруг места происшествия для недопущения посторонних лиц, включая собственников, потерпевших, которые могут изменить данные, изоляция устройств от доступа посторонних лиц, исключение любых манипуляций с оборудованием [3, с. 311–312]; защиты оборудования от дождя, пыли или резких изменений температуры; строгого соблюдения запрета на изменение состояния работающего или выключенного оборудования.

Принцип минимального вмешательства требует от сотрудника полиции пассивной, но крайне ответственной роли по сохранению неприкосновенности «цифровой» обстановки места преступления.

Непринятие мер по изоляции места происшествия ведет к риску утраты или изменения данных. Изъятие цифровых носителей без использования специальных антистатических или экранирующих пакетов может привести к повреждению данных статическим электричеством или удаленному стиранию.

Чаще всего сотрудники полиции, прибывающие первыми на место совершения преступления, обладают базовыми знаниями для охраны места происшествия, но не имеют квалификации и специального оборудования для корректного изъятия цифровых доказательств. Только специалист-криминалист с соответствующей подготовкой в области компьютерной криминалистики или сотрудник специализированного подразделения могут провести осмотр и изъятие цифровых носителей с соблюдением всех процессуальных норм УПК РФ и требований стандартов. Установив, что на месте преступления присутствуют электронные носители информации или преступление совершено удаленно с их использованием, критически важным шагом для обеспечения эффективности расследования является немедленный запрос на выезд специализированного сотрудника. Специалист знает, как работать с энергозависимой информацией, как создавать побитовые копии (образы дисков), применять методы хеширования для обеспечения целостности данных, что гарантирует их юридическую допустимость.

Таким образом, действия сотрудников полиции, первыми прибывающих на место преступления, совершенного с использованием информационно-коммуникационных технологий, по идентификации и сбору сводятся к обнаружению, защите и документированию, что является фундаментом для дальнейшей квалифицированной работы специалистов-криминалистов и следователей, которые уже проводят изъятие и анализ цифровых данных в строгом соответствии с УПК РФ.

Принцип допустимости доказательств – это гарантия законности и справедливости уголовного процесса. Он гарантирует, что обвинение будет основываться только на легитимно полученных данных. В контексте работы с цифровыми доказательствами этот принцип обязывает сотрудников полиции строго следовать процедурам, описанным в ГОСТ Р ИСО/МЭК 27037-2014, для обеспечения юридической силы этих хрупких данных.

Список источников

1. Гетокова Л. Ю. Особенности процессуального документирования административного правонарушения, предусмотренного ст. 7.19 КоАП РФ «самовольное подключение и использование электрической, тепловой энергии, нефти или газа» // Международный академический журнал. 2025. № 3.
2. Коркмазов А. В. Актуальные вопросы деятельности сотрудников полиции по предупреждению правонарушений экстремистской направленности // Теория и практика общественного развития. 2017. № 17.
3. Кучмезов Р. А. Структура способности сотрудников полиции устанавливать доверительные отношения с населением различных категорий // Мир науки, культуры, образования. 2019. № 1 (74).

Библиографический список

1. Kaspersky. Russia Cyber Threat Report 2025. – Moscow, 2026.
2. Голубев, В. И. Киберпреступность в эпоху ИИ: вызовы для правоохранительных органов / В. И. Голубев // Юридическая наука и практика. – 2026. – № 1. – С. 11–20.

Информация об авторах:

Исаева Елена Дмитриевна,
доцент кафедры криминалистики и уголовно-правовых дисциплин;

Зашакуев Азамат Заурович,
преподаватель кафедры деятельности ОВД в особых условиях

About the authors:

Isaeva Elena D.,
associate professor of the department of criminalistics and criminal law disciplines;

Zashakuev Azamat Z.,
lecturer of the department of internal affairs in special conditions

Сведения о вкладе каждого автора

Вклад авторов: *все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.*
Contribution of the authors: *the authors contributed equally to this article. The authors declare no conflicts of interests.*

Статья поступила в редакцию 25.01.2026; одобрена после рецензирования 17.02.2026; принята к публикации 23.03.2026.
The article was submitted to the editorial office 25.01.2026; approved after reviewing 17.02.2026; accepted for publication 23.03.2026.