МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное казенное образовательное учреждение
высшего образования
«Уфимский юридический институт МВД Российской Федерации»

Кафедра криминалистики

ДИПЛОМНАЯ РАБОТА

на тему **«ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ КАК ЭЛЕМЕНТ ТЕХНИКО-КРИМИНАЛИСТИЧЕСКОГО ОБЕСПЕЧЕНИЯ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ (ПО МАТЕРИАЛАМ ТЕРРИТОРИАЛЬНОГО ОРГАНА ВНУТРЕННИХ ДЕЛ)»**

Выполнил
Ширина Иван Владимирович
обучающийся по специальности
40.05.01 Правовое обеспечение
национальной безопасности
2020 года набора, 0101 учебной группы

Руководитель
доцент кафедры криминалистики,
кандидат юридических наук,
Ахметгалеев Вадим Ралифович

К защите рекомендуется
рекомендуется / не рекомендуется
Начальник кафедры _____ Э.Д. Нугаева
подпись
Дата защиты «___»_____2026 г. Оценка_____

ПЛАН

ВВЕДЕНИЕ

Актуальность исследования обусловлена тем, что современное общество пронизано цифровыми технологиями. Правоохранительная система, выполняющая функцию защиты общественного порядка и противодействия преступности, не может оставаться в стороне от данных процессов. Расследование преступлений, как сложная, регламентированная законом деятельность, сегодня немыслимо без применения научно-технических средств, совокупность которых формирует систему технико-криминалистического обеспечения. В структуре данной системы информационно-коммуникационные технологии (далее по тексту – ИКТ) перестали быть лишь вспомогательным инструментом, превратившись в фундаментальный, системообразующий компонент. Изучение ИКТ приобретает особую значимость в контексте стремительной эволюции как самих технологий, так и нормативно-правовой базы, регулирующей их применение.

Традиционная система технико-криминалистического обеспечения, сформировавшаяся в индустриальную эпоху, была ориентирована на работу с материальными, осязаемыми следами преступления. Современная преступная деятельность все чаще реализуется или опосредуется цифровой средой, порождая новый класс криминалистически значимой информации – электронные (цифровые) следы. Подобные следы, обладая свойствами виртуальности, латентности, легкой тиражируемости, ставят перед криминалистической наукой задачу пересмотра и адаптации существующих методик, разработки принципиально новых подходов к их обнаружению, фиксации, изъятию и исследованию.

С практической точки зрения, актуальность темы определяется насущными потребностями следственной и экспертной деятельности. Объем и сложность цифровых данных, связанных с расследуемым событием, растут экспоненциально. Современное расследование требует работы не только с компьютерами и смартфонами, но и с данными облачных сервисов, систем

«умного дома» и других современных устройств. Без адекватных технологических средств и методик, без специалистов, владеющих навыками цифровой криминалистики, извлечение и анализ подобной информации становятся невозможными. Более того, сами ИКТ предоставляют правоохранительным органам мощные аналитические инструменты: системы интеллектуального анализа больших данных для выявления скрытых связей и паттернов преступной деятельности, биометрические идентификационные комплексы, геоинформационные системы для пространственного анализа. Исследование эффективности, границ и оптимальных моделей внедрения указанных инструментов в повседневную практику напрямую влияет на результативность борьбы с преступностью, особенно с ее высокотехнологичными и организованными формами.

Объектом исследования выступает система технико-криминалистического обеспечения расследования преступлений в ее современном состоянии, рассматриваемая в условиях активной цифровизации общества и правоохранительной деятельности.

Предметом исследования являются закономерности, особенности и перспективы интеграции информационно-коммуникационных технологий в указанную систему как ее структурного и функционального элемента, включая возникающие при этом правовые, методические и организационные взаимосвязи.

Цель исследования заключается в комплексном анализе места и роли информационно-коммуникационных технологий в технико-криминалистическом обеспечении, разработке на основе полученных результатов научно-практических рекомендаций по оптимизации их применения в процессе расследования с учетом актуальных требований закона.

Поставленная цель определила решение следующих задач:

- раскрыть понятие, систему и задачи технико-криминалистического обеспечения;

- определить место и роль информационно-коммуникационных

технологий в системе технико-криминалистического обеспечения;

- дать классификацию и характеристику информационно-коммуникационных технологий, используемых на основных этапах расследования;

- выявить актуальные проблемы и перспективы развития использования информационно-коммуникационных технологий в технико-криминалистическом обеспечении.

Методическую основу исследования составили сравнительно-правовой и формально-юридический анализ для изучения нормативной базы, историко-правового метода для ретроспективной оценки развития технологий в криминалистике. Исследование также будет опираться на методы социологического характера, такие как изучение и обобщение следственной и экспертной практики ОМВД России по Белебеевскому району.

Степень разработанности темы исследования. Проблематика применения научно-технических средств в криминалистике традиционно занимает значимое место в трудах отечественных ученых. Вопросы, связанные с использованием компьютерных технологий и цифровых следов, активно разрабатываются в рамках формирующегося направления цифровой криминалистики, чему посвящены исследования ряда современных авторов, рассматривающих технические и процессуальные особенности работы с электронными доказательствами. Однако динамичный характер развития как самих информационно-коммуникационных технологий, так и законодательного поля, их регулирующего, обусловливает наличие определенной лакуны. Зачастую научные работы концентрируются на узкопрофессиональных задачах компьютерно-технической экспертизы, тогда как системный взгляд на ИКТ именно как на сквозной, преобразующий элемент всей системы технико-криминалистического обеспечения, ее организационных и тактических моделей в свете последних правовых изменений, представлен в литературе недостаточно полно.

Теоретическую базу исследования составили фундаментальные

положения общей теории криминалистики, научные труды в области криминалистической техники и тактики, специальные работы по цифровой криминалистике, теории операций и систем, теории информации, а также публикации, затрагивающие философские и социальные последствия технологизации права.

Нормативную основу работы образует комплекс законодательных и подзаконных актов Российской Федерации. В эту группу входят Конституция РФ, уголовно-процессуальное законодательство, федеральные законы, регулирующие вопросы оперативно-розыскной деятельности, защиты персональных данных, информационной безопасности, связи, а также системы государственных информационных систем.

Эмпирическая база исследования сформирована из материалов опубликованной судебной и следственной практики по делам, связанным с использованием цифровых доказательств, данных официальной статистики правоохранительных органов, открытых аналитических отчетов и обзоров технологических компаний в сфере информационной безопасности.

Практическая значимость исследования определяется его ориентацией на решение актуальных проблем, стоящих перед органами предварительного расследования и судебно-экспертными учреждениями. Результаты работы могут быть использованы для совершенствования методических рекомендаций по обнаружению, изъятию и исследованию цифровых следов, организации взаимодействия между участниками процесса при работе с электронными доказательствами.

Структура работы определена целью и задачами исследования и состоит из введения, двух глав, включающих четыре параграфа, заключения и списка использованной литературы.

ГЛАВА 1. ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ ТЕХНИКО-КРИМИНАЛИСТИЧЕСКОГО ОБЕСПЕЧЕНИЯ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

§ 1. Понятие, система и задачи технико-криминалистического обеспечения

Современное состояние борьбы с преступностью характеризуется сложным переплетением традиционных криминальных проявлений и новых форм противоправной деятельности, порожденных научно-техническим прогрессом. В подобных условиях эффективность правоохранительной системы в значительной мере определяется развитостью ее научно-технического фундамента. Таким фундаментом выступает технико-криминалистическое обеспечение (далее по тексту – ТКО), представляющее собой сложную, динамично развивающуюся подсистему криминалистики и практической деятельности по раскрытию и расследованию преступлений.

Осмысление его сущности, внутреннего устройства и целевого назначения является необходимым условием для адекватного ответа на вызовы, связанные с усложнением способов совершения преступлений и появлением новых видов доказательств. Данное осмысление приобретает особую глубину в контексте цифровой трансформации общества, требующей пересмотра и адаптации многих устоявшихся криминалистических концепций.

Понятие технико-криминалистического обеспечения формировалось исторически, параллельно с развитием самой криминалистической науки. Изначально оно сводилось преимущественно к совокупности средств и методов работы со следами, основанных на достижениях естественных и технических наук. Однако по мере усложнения задач расследования и расширения арсенала научно-технических инструментов, понимание данного феномена углубилось[1].

---

[1] Брезгулевская А.А., Шлапакова В.А. Информационные системы и технологии в криминалистике: как компьютерный прогресс повлиял на уголовные расследования // Современные вопросы устойчивого развития общества в эпоху трансформационных процессов: сборник научных трудов. М., 2023. С. 146.

Технико-криминалистическое обеспечение связано с криминалистической техникой как разделом криминалистики. Сам термин «обеспечение» возможно определять в двух взаимосвязанных аспектах: во-первых, это физическое наличие технических средств, методик, технологий, необходимой информации и, во-вторых, выполнение поставленных задач и достижение целей путем проведения конкретных организационных мероприятий и осуществления соответствующей деятельности. В современной криминалистике наиболее авторитетным признано мнение, что под криминалистическим обеспечением деятельности органов внутренних дел в целом понимается система криминалистических знаний и основанных на них навыков и умений использовать научные криминалистические рекомендации, применять криминалистические средства, методы и технологии их использования в целях предотвращения, выявления, раскрытия и расследования преступлений[1].

Криминалистическое обеспечение – это система, т.е. определенный порядок, нечто целое, представляющее собой единство находящихся во взаимной связи частей, поскольку при современном высоком уровне развития науки и техники необходим, полагаем, и комплексный, системный подход к решению поставленных задач. Безусловно, данная система надлежащим образом организована (прежде всего, на основе современных достижений науки) и функционирует, используя технические средства, соответствующие методы и методики для достижения определенной цели – способствование поддержанию правопорядка, обеспечению законности. Причем эта система функционирует в тех или иных правовых рамках, т.к. ее деятельность регулируется соответствующими нормативными актами (например, использование специальных знаний строго регламентируется УПК РФ). Криминалистическое обеспечение в целом как система снабжает данный

[1] Рахмонбердиев Б.Б. Применение информационных технологий в органах предварительного расследования // Уголовное судопроизводство России и зарубежных государств: проблемы и перспективы развития: сборник научных трудов. Санкт-Петербург, 2023. С. 659.

процесс криминалистически значимой, в том числе и доказательственной, информацией способствуя соблюдению законности.

В современном научном представлении технико-криминалистическое обеспечение можно определить как целенаправленную, системно организованную деятельность, которая включает в себя разработку, производство, внедрение и применение специальных технических средств, методов и методик для решения задач уголовного судопроизводства, а также научные исследования, обеспечивающие развитие этого арсенала. Данная деятельность не является самоцелью; ее смысл заключается в служении целям правосудия – установлению истины по делу посредством обнаружения, фиксации, исследования и использования криминалистически значимой информации.

Таким образом, понятие охватывает не только материальную составляющую в виде приборов и реагентов, но и интеллектуальную – знание о закономерностях возникновения следов и алгоритмах работы с ними.

Значительный интерес при изучении вопросов правового обеспечения представляют принципы применения технико-криминалистических средств (далее по тексту – ТКС), к которым принято относить: 1) правомерность их использования; 2) научная обоснованность; 3) соблюдение прав личности; 4) безопасность; 5) эффективность; 6) применение технических средства ограниченным законом кругом лиц; 7) сохранность исследуемого объекта; 8) экономичность, т.е. применение технических средств с наименьшими затратами сил и средств[1].

Применение технических средств в рамках оперативно-розыскной деятельности должно соответствовать данным принципам. Однако, думается, что принцип сохранения исследуемого объекта в рамках оперативно-розыскной деятельности (далее по тексту – ОРД) должен быть факультативным.

---

[1] Амиров Р.Г., Еремченко В.И. Проблемы использования современных информационных технологий в расследовании преступлений // Евразийский юридический журнал. 2023. № 11. С. 365.

Действительно, если нет необходимости, например, в дальнейшем (экспертном) исследовании какого–либо вещества или возврате владельцу, то допустимо это вещество при исследовании расходовать полностью.

Система технико-криминалистического обеспечения, будучи подсистемой криминалистики, обладает собственным внутренним строением, элементами которого выступают взаимосвязанные компоненты. Традиционно в структуре системы выделяют несколько базовых направлений или блоков. Один из таких блоков связан с криминалистической техникой – разделом криминалистики, изучающим закономерности возникновения и существования материальных следов преступления и разрабатывающим технические средства, приемы и методики для работы с ними. Сюда входят средства и методы обнаружения, фиксации и изъятия следов (фотография, видеозапись, 3D-сканирование, измерительные инструменты), трасология, судебная баллистика, исследование документов, габитоскопия, фоноскопия и другие виды традиционных криминалистических экспертиз. Другой важнейший блок составляет криминалистическая тактика, которая, хотя и направлена на разработку рекомендаций по организации и планированию расследования, тактике следственных действий, тесно переплетается с техническим обеспечением. Любое современное следственное действие – будь то осмотр, обыск, следственный эксперимент или предъявление для опознания – требует применения технических средств для объективной фиксации его процесса и результатов[1].

Особое место в системе занимает формирование и использование криминалистических учетов и коллекций. Данный компонент представляет собой информационную основу технико-криминалистического обеспечения. Создание и ведение автоматизированных банков данных по пулям и гильзам, дактилоскопической информации, поддельным денежным знакам и документам, методикам совершения преступлений позволяет осуществлять

[1] Селютин Д.М. Методология использования информационных технологий в расследовании преступлений // Молодой ученый. 2025. № 3. С. 17.

розыск, устанавливать серийность преступлений и идентифицировать объекты. В эпоху цифровизации данный блок претерпевает наиболее радикальные изменения, трансформируясь в сложные межведомственные информационно-аналитические системы, работающие с большими массивами структурированных и неструктурированных данных.

Отдельным, стремительно развивающимся структурным элементом системы выступает цифровая (компьютерная) криминалистика. Появление данного направления стало закономерной реакцией на распространение компьютерных технологий и рост киберпреступности. Цифровая криминалистика занимается разработкой средств и методов обнаружения, изъятия, сохранения, анализа и представления цифровых доказательств, хранящихся на электронных носителях или передаваемых по сетям. Ее интеграция в общую систему технико-криминалистического обеспечения носит двоякий характер: с одной стороны, она представляет собой специализированный блок, обладающий своей специфической методологией; с другой – ее технологии пронизывают все остальные блоки, модифицируя традиционные методики (например, использование цифровой фотограмметрии в трасологии или спектрального анализа в исследовании веществ).

Наконец, неотъемлемой частью системы является научно-исследовательская и организационно-управленческая деятельность. Она включает в себя прогнозирование потребностей практики, планирование и проведение прикладных научных исследований, разработку и стандартизацию новых технических средств и методик, подготовку кадров, организацию производства и снабжения правоохранительных органов необходимым оборудованием, а также координацию взаимодействия между следственными, оперативными и экспертными подразделениями[1].

Задачи технико-криминалистического обеспечения вытекают

[1] Казакова В.С. Роль информационных технологий при расследовании преступлений // Научный поиск курсантов: сборник научных трудов. Могилев, 2025. С. 96.

непосредственно из его целей и системного устройства. Их можно разделить на несколько взаимосвязанных групп. Фундаментальной задачей, лежащей в основе всех остальных, является разработка теоретических основ и методологических принципов создания и применения криминалистической техники. Без глубокого научного изучения закономерностей возникновения следов, физико-химических процессов, возможностей современных аналитических приборов невозможно создание эффективных практических инструментов.

На основе теоретических изысканий решается прикладная задача создания конкретных технических средств, приемов и методик для работы с различными видами доказательств. Данная задача носит непрерывный, эволюционный характер, поскольку преступная среда постоянно адаптируется и изобретает новые способы сокрытия следов. Ответом должно стать опережающее развитие криминалистических технологий. Особую остроту в настоящее время приобретает задача разработки комплексных методик работы со смешанными, гибридными следами, сочетающими материальные и цифровые компоненты, например, при расследовании преступлений, где физическое воздействие (убийство, кража) подготавливается и координируется через зашифрованные мессенджеры, а материальные ценности обналичиваются через криптовалютные кошельки[1].

Важнейшей практической задачей выступает непосредственное применение разработанного арсенала в процессе предварительного расследования и судебного разбирательства. Эта задача включает в себя обучение следователей, дознавателей, оперативных работников и судей правильному использованию технических средств, формирование у них криминалистического мышления, позволяющего грамотно выдвигать версии о механизме преступления и возможных следах. От того, насколько качественно и процессуально корректно будут применены технико-

[1] Ардавов М.М. О проблемных аспектах применения информационных технологий в расследовании преступлений // Право и управление. 2025. № 7. С. 132.

криминалистические средства на месте происшествия, зависит сохранность и допустимость будущих доказательств.

В условиях информационного общества на первый план выходит задача формирования и эффективной эксплуатации интегрированных криминалистических учетов и информационно-поисковых систем. Актуальность данной задачи усиливается с принятием законодательных актов, расширяющих возможности государственной геномной регистрации, биометрического учета и межведомственного электронного взаимодействия. Речь идет уже не просто о создании баз данных, а о построении аналитических платформ, способных с помощью технологий больших данных и искусственного интеллекта выявлять скрытые связи, прогнозировать криминальные тенденции и поддерживать принятие решений.

Отдельного внимания заслуживает задача правовой регламентации и стандартизации применения технико-криминалистических средств. Появление новых технологий, таких как дистанционное зондирование, применение беспилотных летательных аппаратов для осмотра местности, использование алгоритмов распознавания лиц в публичных пространствах, требует четкого законодательного закрепления условий и пределов их правомерного использования в уголовном процессе. Последние инициативы российского законодателя в сфере регулирования оборота данных, систем видеонаблюдения и биометрии формируют новые правовые рамки, внутри которых должно развиваться технико-криминалистическое обеспечение[1].

Наконец, стратегической задачей является кадровое и ресурсное обеспечение всей системы. Она подразумевает не только подготовку высококвалифицированных экспертов и криминалистов, владеющих междисциплинарными знаниями на стыке юриспруденции, информатики и естественных наук, но и создание устойчивой инфраструктуры – от специализированных лабораторий до центров коллективного пользования

[1] Архипова П.С. Отдельные проблемы использования информационных технологий в расследовании преступлений // Студенческий вестник. 2024. № 11. С. 20.

уникальным аналитическим оборудованием.

В организационных основах системы ТКО раскрытия и расследования преступлений структурными составляющими являются два элемента – организационно-управленческий (организационно-кадровый, организационно–штатный), связанный с деятельностью организации (учреждения), и организационно-функциональный (организационно-технический), связанный с применением технико-криминалистических средств[1].

Таким образом, технико-криминалистическое обеспечение представляет собой сложную, открытую и динамичную систему. Ее понятие охватывает единство научной, производственной и практической деятельности, направленной на вооружение субъектов уголовного судопроизводства научно-техническими средствами познания обстоятельств преступления. Система данного обеспечения структурно многокомпонентна, объединяя традиционные разделы криминалистической техники, современные цифровые методики, информационные ресурсы и управленческие механизмы. Задачи, стоящие перед системой, носят многоуровневый характер: от фундаментальных научных исследований до прикладного внедрения и правовой легитимации новых технологий.

Успешное функционирование и развитие технико-криминалистического обеспечения в современных условиях является непременным условием обеспечения законности, обоснованности и справедливости правосудия, способности государства эффективно противостоять преступности как в реальном, так и в виртуальном пространстве. Постоянная адаптация этой системы к технологическим и правовым новшествам определяет ее жизнеспособность и практическую ценность.

[1] Губарева А.С. Перспективы и риски использования информационных технологий при расследовании преступлений // Научный альманах. 2025. № 6. С. 72.

§ 2. Место и роль информационно-коммуникационных технологий в системе технико-криминалистического обеспечения

Современный этап общественного развития неразрывно связан с процессами глубокой цифровизации, которые затрагивают все без исключения социальные институты. Правоохранительная система и, в частности, ее научно-технический фундамент – технико-криминалистическое обеспечение – переживают в связи с указанными процессами период фундаментальной трансформации.

Информационно-коммуникационные технологии перестали выполнять сугубо вспомогательную функцию, превратившись в стержневой элемент самой парадигмы раскрытия и расследования преступлений. Их внедрение и развитие происходит в условиях динамично меняющегося правового поля, где последние законодательные инициативы Российской Федерации, направленные на регулирование цифрового пространства, защиты данных и обеспечения кибербезопасности, задают новые векторы и устанавливают необходимые правовые границы. Поэтому осмысление места и роли ИКТ в технико-криминалистическом обеспечении требует комплексного анализа, учитывающего не только технологический потенциал, но и его правовое опосредование[1].

Исторически сложившаяся система технико-криминалистического обеспечения всегда являлась ответом криминалистической науки и практики на эволюцию преступных проявлений. Появление новых видов преступной деятельности, связанных с использованием компьютерной техники, сетевых коммуникаций и цифровых данных, породило качественно иной тип криминалистически значимой информации – электронные следы. Подобные следы, в отличие от традиционных вещественных доказательств,

---

[1] Береза К.Ю. Использование искусственного интеллекта и информационных технологий в ходе расследования уголовных дел // Государство, право, экономика: история и современность: сборник научных трудов. Краснодар, 2025. С. 70.

нематериальны, легко тиражируемы, модифицируемы и могут быть мгновенно трансгранично перемещены. Данное обстоятельство поставило перед криминалистикой задачу разработки принципиально новых методов работы, что привело к формированию отдельного научно-практического направления – цифровой (компьютерной) криминалистики. Однако сегодня влияние ИКТ вышло далеко за пределы данного направления, проникнув во все традиционные разделы криминалистической техники и тактики, что свидетельствует о системной интеграции технологий.

Место ИКТ в рассматриваемой системе определяется их инфраструктурной функцией. Речь идет о создании единого информационно-аналитического пространства, объединяющего разрозненные массивы данных, ресурсы и службы. Формирование государственных информационных систем криминалистической и оперативно-справочной направленности, таких как автоматизированные дактилоскопические идентификационные системы, базы данных по пулям и гильзам, регистры геномной информации, было бы невозможным без мощных серверных комплексов, специализированного программного обеспечения и защищенных каналов передачи данных.

Последние изменения в законодательстве, в частности, касающиеся порядка обработки биометрических персональных данных и функционирования системы государственной геномной регистрации, не только расширяют возможности таких систем, но и накладывают строгие требования по обеспечению конфиденциальности и безопасности хранимой информации. Таким образом, ИКТ формируют технологический базис для централизованного хранения, обработки и анализа криминалистических учетов, превращая их из статических архивов в динамичные инструменты для установления связей между расследуемыми событиями[1].

Роль информационно-коммуникационных технологий в практической

[1] Амиров Р.Г., Еремченко В.И. Проблемы использования современных информационных технологий в расследовании преступлений // Евразийский юридический журнал. 2023. № 11. С. 366.

деятельности по раскрытию преступлений проявляется многообразно. На стадии обнаружения и фиксации следов применяются не только цифровые фото- и видеоаппаратура, но и трехмерное сканирование места происшествия, позволяющее создать его точную виртуальную модель для последующего неоднократного изучения.

Средства мобильной связи и навигации подозреваемых лиц, данные с видеорегистраторов и камер городского наблюдения, в том числе использующих алгоритмы распознавания лиц и автомобильных номеров, стали стандартными источниками доказательственной информации. Правовое регулирование использования подобных технологий, например, порядок получения сведений от операторов связи или применения систем видеонаблюдения с функцией биометрической идентификации, постоянно уточняется, что отражает поиск баланса между эффективностью расследования и защитой прав граждан.

Экспертная криминалистическая деятельность также претерпела радикальные изменения благодаря ИКТ. Современные программно-аппаратные комплексы для исследования компьютерных носителей позволяют проводить глубокий анализ файловых систем, восстанавливать удаленные данные, изучать журналы событий и сетевую активность. При исследовании традиционных объектов – документов, волокон, следов выстрела – применяются приборы с цифровой обработкой сигналов и автоматизированным сравнением полученных изображений с базами данных[1].

Технологии искусственного интеллекта, в частности машинное обучение, начинают использоваться для решения задач, связанных с анализом больших массивов однотипных данных, например, при классификации следов или первичном отборе совпадений в дактилоскопических базах. Однако применение подобных алгоритмов, особенно в контексте принятия процессуальных решений, требует особой правовой регламентации

[1] Кислицына А.Е., Зятюк Б.И. Методология использования информационных технологий в расследовании // Моя профессиональная карьера. 2025. № 71. С. 166.

и методологической проработки, поскольку результат работы машины должен быть верифицируем и понятен для участников судопроизводства.

Отдельного внимания заслуживает роль ИКТ в борьбе с преступлениями, совершаемыми в цифровой среде. Киберпреступность, финансирование терроризма, распространение экстремистских материалов в сети «Интернет» – все эти виды противоправной деятельности порождают специфические цифровые следы, требующие специальных методов обнаружения и исследования.

Законодательные новеллы, направленные на противодействие таким угрозам, например, нормы, обязывающие организаторов распространения информации в сети обеспечивать хранение данных о фактах приема, передачи и обработки голосовой информации и текстовых сообщений, напрямую формируют запрос на соответствующие криминалистические технологии. Разработка средств для мониторинга сетевого трафика, анализа деструктивного контента, раскрытия анонимности пользователей, работа в даркнете становится обязательным компонентом арсенала следственных подразделений. Происходит постоянное соревнование технологий защиты и нападения в киберпространстве, что стимулирует развитие криптографии, стеганографии и средств противодействия им в рамках судебных экспертиз[1].

Важнейшим проявлением интеграции ИКТ стала трансформация организации управления расследованием. Внедрение специализированных информационных систем управления делами позволяет координировать работу следственно-оперативных групп, планировать мероприятия, контролировать сроки и хранить всю документацию по делу в электронном виде. Системы электронного документооборота и межведомственного взаимодействия ускоряют получение необходимых справок и заключений. Дистанционные технологии, получившие особый импульс развития в последние годы, находят

[1] Таашев Д.Б. Проблемные аспекты применения информационных технологий в расследовании преступлений в цифровом пространстве // Российский научный вестник. 2025. № 4. С. 253.

применение при проведении отдельных следственных действий, например, допросов свидетелей или участия специалистов в осмотре места происшествия посредством видеоконференц-связи. Подобные практики требуют четкой процессуальной фиксации для гарантии соблюдения прав участников процесса и достоверности полученных показаний.

Несмотря на очевидные преимущества, широкое внедрение ИКТ порождает комплекс проблем, определяющих направления для дальнейшего совершенствования системы технико-криминалистического обеспечения. Правовые сложности связаны с тем, что скорость технологических изменений зачастую опережает темпы законотворчества. Вопросы, связанные с юрисдикцией при получении данных из облачных хранилищ, расположенных за рубежом, правомерностью использования хакерских инструментов в оперативно-розыскной деятельности, допустимостью доказательств, полученных с помощью автоматизированных алгоритмов прогнозной аналитики, остаются дискуссионными.

Российский законодатель, принимая законы в сфере цифровой экономики и противодействия киберугрозам, стремится создать правовые основания для применения передовых технологий, одновременно устанавливая барьеры от их злоупотребления. Технические вызовы обусловлены постоянным усложнением аппаратно-программных экосистем, распространением сквозного шифрования, появлением новых типов устройств (Интернет вещей), что требует непрерывного обновления парка технических средств и методик экспертного исследования[1].

Кадровое обеспечение представляет собой отдельную масштабную задачу. Современный криминалист или следователь должен обладать не только глубокими юридическими знаниями, но и цифровой грамотностью, понимать основы работы с цифровыми следами. Подготовка экспертов в области компьютерной криминалистики требует междисциплинарного подхода,

[1] Архипова П.С. Отдельные проблемы использования информационных технологий в расследовании преступлений // Студенческий вестник. 2024. № 11. С. 21.

сочетающего программирование, теорию информации и уголовно-процессуальное право. Инвестиции в образование и непрерывное профессиональное обучение являются необходимым условием эффективного использования технологического потенциала.

Использование информационно-коммуникационных технологий в практической деятельности Отдела МВД России по Белебеевскому району осуществляется по ряду направлений технико-криминалистического обеспечения расследования преступлений. В настоящее время сотрудники районного отдела применяют имеющиеся цифровые средства в повседневной работе, однако уровень их использования характеризуется неравномерностью: отдельные направления относительно развиты, тогда как потенциал многих современных технологий реализуется лишь фрагментарно или не используется вовсе.

При производстве осмотров мест происшествий сотрудники следственно-оперативных групп Белебеевского ОМВД используют цифровые фотоаппараты для фиксации обстановки. Фотосъемка осуществляется с целью последующего приобщения снимков к материалам уголовных дел в качестве приложений к протоколам. В распоряжении выезжающих на место происшествия сотрудников имеются портативные цифровые камеры, позволяющие получать изображения удовлетворительного качества. Однако применение более совершенных технологий фиксации, таких как панорамная съемка или трехмерное моделирование места происшествия, в практике отдела отсутствует ввиду отсутствия соответствующего оборудования и специалистов, владеющих данными методиками.

Для фиксации хода следственных действий применяется видеозапись. Наиболее часто она используется при проведении проверок показаний на месте, следственных экспериментов и допросов несовершеннолетних потерпевших, что прямо предусмотрено уголовно-процессуальным законодательством. В распоряжении отдела имеются портативные видеокамеры, однако их количество ограничено, а технические характеристики не всегда позволяют

получать качественную запись в условиях недостаточной освещенности или на открытой местности. Систематическое применение видеозаписи при иных следственных действиях, где она могла бы повысить доказательственное значение получаемых материалов, не сложилось в устойчивую практику.

При работе с базами данных и криминалистическими учетами сотрудники Белебеевского ОМВД используют автоматизированные информационно-поисковые системы, функционирующие в единой системе информационно-аналитического обеспечения МВД России. Доступ к федеральным базам данных, включая интегрированный банк данных федерального уровня, осуществляется через защищенные каналы связи. При проверке лиц по оперативно-справочным учетам, установлении их причастности к ранее совершенным преступлениям, наличии судимостей, а также при проверке транспортных средств и похищенного имущества сотрудники направляют запросы через ведомственные информационные системы. Вместе с тем, возможности углубленного анализа имеющейся информации, выявления скрытых связей между лицами и событиями используются недостаточно, что обусловлено как ограниченным функционалом доступных на районном уровне систем, так и недостаточной подготовкой сотрудников в области информационной аналитики.

При изъятии электронных носителей информации, таких как компьютеры, ноутбуки, мобильные телефоны, сотрудники руководствуются общими требованиями уголовно-процессуального законодательства об обеспечении сохранности доказательств. Изъятые носители упаковываются с соблюдением правил, исключающих возможность доступа к информации и ее повреждения при транспортировке. Однако специальные аппаратно-программные комплексы для предварительного исследования содержимого электронных устройств непосредственно на месте происшествия в подразделении отсутствуют. В связи с этим все изъятые носители направляются для производства экспертиз в Экспертно-криминалистический центр МВД по Республике Башкортостан, расположенный в городе Уфе, что

приводит к значительным временным задержкам, поскольку сроки производства таких экспертиз могут составлять несколько месяцев.

В оперативно-розыскной деятельности сотрудники используют возможности мониторинга открытых источников информации. При отработке лиц, представляющих оперативный интерес, осуществляется проверка наличия и активности их аккаунтов в социальных сетях, изучается размещаемая информация, круг общения. Однако данная работа проводится бессистемно, без использования специализированного программного обеспечения для анализа открытых данных, и во многом зависит от личной инициативы конкретных сотрудников и их навыков работы с интернет-ресурсами.

При расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий, сотрудники взаимодействуют с банковскими учреждениями и операторами сотовой связи. Запросы о предоставлении информации о движении денежных средств и соединениях абонентов направляются преимущественно на бумажных носителях, что замедляет получение ответов. Электронное межведомственное взаимодействие развито недостаточно, хотя техническая возможность направления запросов в электронном виде по отдельным направлениям существует.

Для внутреннего документооборота и обмена информацией между сотрудниками используется ведомственная электронная почта, функционирующая в защищенной сети передачи данных. Через систему электронного документооборота осуществляется регистрация входящей и исходящей корреспонденции, направление поручений и контроль их исполнения. Вместе с тем, значительная часть информации по-прежнему дублируется на бумажных носителях, что связано как с требованиями ведомственных инструкций, так и с привычкой сотрудников к традиционным формам работы.

Видеоконференцсвязь используется для участия в совещаниях, проводимых руководством МВД по Республике Башкортостан, а также для

взаимодействия с судами при рассмотрении ходатайств об избрании мер пресечения в случаях, когда доставление подозреваемого в суд затруднено. Оборудование для видеоконференцсвязи в отделе имеется и функционирует, однако используется преимущественно по указанию вышестоящего руководства, а не в инициативном порядке для решения повседневных задач взаимодействия с другими подразделениями.

При назначении и производстве судебных экспертиз взаимодействие с Экспертно-криминалистическим центром осуществляется посредством направления постановлений и сопроводительных писем. Часть документов направляется в электронном виде, однако окончательные заключения экспертов поступают на бумажных носителях, что сохраняет необходимость их физической доставки. Электронные копии заключений используются редко и не имеют самостоятельного доказательственного значения.

Для обеспечения доступа к актуальным нормативным правовым актам сотрудники используют справочно-информационные системы, установленные на служебных компьютерах. Обновление этих систем производится централизованно, однако периодичность обновления не всегда обеспечивает наличие самых последних редакций документов, что требует от сотрудников дополнительной проверки информации через официальные источники.

Средства криптографической защиты информации установлены на служебных компьютерах, подключенных к ведомственной сети. Доступ к информационным ресурсам осуществляется с использованием электронных ключей и паролей. Передача информации, содержащей персональные данные или составляющей служебную тайну, осуществляется по защищенным каналам. Вместе с тем, многоступенчатые процедуры доступа и ограничения на передачу данных нередко побуждают сотрудников использовать для оперативной коммуникации личные средства связи и неофициальные каналы, что создает риски утечки служебной информации.

При расследовании дорожно-транспортных происшествий сотрудники используют данные с камер видеонаблюдения, установленных на улицах

города Белебей и на трассах. Запросы в организации, осуществляющие эксплуатацию камер, направляются по мере необходимости. Однако отсутствие единой системы доступа к муниципальным и частным системам видеонаблюдения вынуждает направлять отдельные запросы по каждой организации, что требует времени и не всегда позволяет получить записи до истечения сроков их хранения.

В дежурной части отдела функционирует автоматизированная система управления нарядами, позволяющая отслеживать местонахождение патрульных автомобилей. Система используется для оперативного направления ближайших нарядов на места происшествий, однако ее аналитические возможности для прогнозирования криминогенной обстановки и оптимизации расстановки сил не задействованы. Система видеонаблюдения, установленная в здании отдела и на прилегающей территории, используется для обеспечения безопасности и фиксации событий, происходящих в административном здании, но записи используются преимущественно для разбора конфликтных ситуаций.

При работе с обращениями граждан используется автоматизированная система учета, в которой фиксируются все этапы движения заявления от момента поступления до принятия процессуального решения. Система позволяет контролировать сроки рассмотрения, назначать исполнителей, отслеживать полноту проводимых проверок. Граждане имеют возможность направить обращение в электронном виде через официальный сайт МВД по Республике Башкортостан, однако доля таких обращений невелика, и они рассматриваются в том же порядке, что и письменные.

Таким образом, использование информационно-коммуникационных технологий в Отделе МВД России по Белебеевскому району в настоящее время ограничивается преимущественно базовыми функциями фиксации, поиска информации и документооборота. Более сложные и перспективные направления, включающие аналитическую обработку данных, предварительное исследование цифровых следов на месте происшествия, системный мониторинг открытых источников и межведомственное электронное взаимодействие,

развиты недостаточно. Основными причинами сложившейся ситуации являются ограниченность материально-технической базы, дефицит подготовленных кадров и отсутствие системного подхода к внедрению технологий в повседневную следственную практику.

Можно сказать, что информационно-коммуникационные технологии заняли центральное место в архитектуре современного технико-криминалистического обеспечения, превратившись из инструментария в среду существования и развития всей системы. Их роль является всепроникающей и преобразующей: ИКТ определяют новые источники и виды доказательств, модифицируют традиционные методики, создают основу для интеллектуальных систем поддержки принятия решений и кардинально меняют организацию процесса расследования. Развитие данного процесса происходит в тесной взаимосвязи с эволюцией законодательной базы, которая стремится обеспечить легитимность применения технологий, защиту прав личности и национальную кибербезопасность.

Будущее технико-криминалистического обеспечения видится в дальнейшей конвергенции цифровых и традиционных криминалистических знаний, в создании гибких, адаптивных систем, способных отвечать на вызовы стремительно цифровизирующегося мира, где граница между реальным и виртуальным пространством становится все более условной. Успех в данном направлении зависит от слаженного взаимодействия законодательной власти, правоохранительных органов, научного сообщества и разработчиков технологических решений.

ГЛАВА 2. ПРИМЕНЕНИЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ПРОЦЕССЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

§ 1. Классификация и характеристика информационно-коммуникационных технологий, используемых на основных этапах расследования

Современный этап общественного развития характеризуется стремительной цифровизацией всех сфер человеческой деятельности, что не могло не оказать глубокого трансформирующего влияния на криминалистическую науку и следственную практику. Информационно-коммуникационные технологии (ИКТ) перестали быть лишь вспомогательным инструментом, превратившись в неотъемлемую среду существования как самого преступного поведения, так и деятельности по его раскрытию и расследованию. Широкое проникновение цифровых технологий в повседневную жизнь привело к образованию новой, гибридной реальности, где материальные и электронные следы преступления тесно переплетены. Данное обстоятельство предъявляет качественно новые требования к методологии расследования, диктуя необходимость системного анализа классификации и функциональных возможностей ИКТ, адаптированных к задачам каждого процессуального этапа[1].

Согласно ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», информационные технологии (далее по тексту – ИТ) – это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. ИТ в

[1] Асылбек Д.Е., Тилеубергенов Е.М. Использование новых информационных технологий при раскрытии и расследовании преступлений // Трансформация российской науки в эпоху информационного общества: сборник научных трудов. М., 2025. С. 155.

настоящее время повсеместно используются при работе с информацией в различных сферах деятельности (экономике, образовании, энергетике и т.д.).

Качественное расследование преступления невозможно без использования технических средств и достижений в области ИТ. ИТ в расследовании преступлений – это совокупность приемов и методов сбора, обработки, хранения, представления и использования криминалистически значимой информации, с применением специальных средств (компьютеры, ноутбуки, смартфоны, программное обеспечение, компьютерные сети и др.), направленных на принятие следователем организационных, тактических и методических решений с их последующей реализацией, обеспечивающей достижение целей расследования.

На современном этапе развития общества происходит интенсивное внедрение ИТ (базовых и прикладных) в различные сферы деятельности, в том числе в деятельность по раскрытию и расследованию преступлений, причем происходят не отдельные акты внедрения ИТ, а комплексное построение цифровой системы в масштабах всей страны. ИТ позволяют оптимизировать деятельность по расследованию преступлений за счет повышения эффективности работы с информацией (ее поиском, сбором, хранением, обработкой, предоставлением и использованием).

Среди ученых существуют различные точки зрения на основные направления использования ИТ в расследовании преступлений. Авторы учебника «Цифровая криминалистика» указывают следующие направления использования ИТ в правоохранительных органах: 1) автоматизированные системы обработки данных; 2) автоматизированные информационно-поисковые системы; 3) автоматизированные информационно-справочные системы; 4) автоматизированные рабочие места; 5) автоматизированные системы управления; 6) экспертные (информационно-аналитические и рекомендующие) системы[1]. П.А. Суетина выделяет шесть направлений использования

[1] Цифровая криминалистика: учеб. для вузов / В.Б. Вехов и др. М.: Юрайт, 2021. С. 26.

компьютерных технологий в расследовании и раскрытии преступлений: 1) автоматизированные системы управления и автоматизированные рабочие места; 2) информационно-справочные системы; 3) экспертно-консультирующие системы; 4) расчетно-аналитические системы; 5) информационные обучающие системы; 6) программы обработки изображений[1]. Следует отметить соотношение понятий: «компьютерные технологии», «информационные технологии» и «цифровые технологии». Цифровые технологии – технологии сбора, хранения, обработки, поиска, передачи и представления данных в электронном виде. Компьютерные технологии, а также информационные технологии – это обобщенное название технологий, отвечающих за хранение, передачу, обработку, защиту и воспроизведение информации с использованием компьютеров. Соответственно эти понятия тождественны.

Соглашаясь с указанными направлениями использования ИТ в расследовании попытаемся упорядочить и конкретизировать их. Как справедливо отмечает Л.Р. Шигапова «задача цифровых технологий, используемых в деятельности правоохранительных органов по раскрытию и расследованию преступлений – адаптировать существующие базовые алгоритмы работы с информацией для решения задач криминалистической деятельности»[2]. Поэтому в предложенной нами классификации возьмем за основание составные части (аспекты) деятельности по расследованию преступлений (познавательный, удостоверительный, организационный):

1) использование ИТ для поиска, обнаружения, изъятия и фиксации криминалистически значимой информации при производстве следственных действий и ее предварительное исследование:

– цифровые технические средства поиска следов преступления. Здесь следует отметить, что процесс научно-технического развития позволил,

---

[1] Суетина П.А. Использование информационно-коммуникационных технологий в расследовании преступлений // Современные достижения молодых исследователей: сборник научных трудов. Пенза, 2023. С. 89.

[2] Шигапова Л.Р. Применение современных информационных технологий на этапе предварительного расследования // Моя профессиональная карьера. 2023. № 55. С. 208.

повысить производительность и эффективность традиционных технических средств (эндоскоп, георадар, газоанализатор и др.), путем их модернизации: а) оснащение данных приборов экраном (дисплеем), что позволяет визуально в режиме онлайн отслеживать осуществление поисковой деятельности; б) наличие программного обеспечения, позволяющего регулировать настройки технического средства в зависимости от особенностей исследуемой обстановки, а также проводить измерения обнаруженных следов (размер, расстояние между объектами, масса и т.д.); в) безотлагательный ввод обнаруженных данных в компьютер, смартфон и т.д.;

– общедоступные ИТ технологии поиска ориентирующей информации о человеке в открытых ресурсах сети Интернет;

– ИТ поиска цифровой информации (цифровых следов). К таковым могут относиться программные и программно-аппаратные технические средства, направленные на выявление и извлечение этой информации из мобильных телефонов, смартфонов, карманных персональных компьютеров, персональных компьютеров, облачных сервисов и др. преодолевая при этом средства их защиты. С этой целью, как отмечает И.В. Семенова, используются программно-аппаратные комплексы: Cellebrite UFED, «МОБИЛЬНЫЙ КРИМИНАЛИСТ ЭКСПЕРТ ПЛЮС», «МОБИЛЬНЫЙ КРИМИНАЛИСТ ДЕСКТОП» и др.[1];

– наиболее широко в настоящее время для фиксации следов и обнаруженной информации, а также хода следственных действий применяется цифровая фото- и видеосъемка, а также звукозапись;

– использование программ конвертации речи в текстили транскрайберов (устройств, позволяющее значительно ускорить документирование звукозаписей и видеозаписей);

– адаптация и последующее повсеместное использование «иных технологий» для фиксации в процессе производства следственных действий,

[1] Семенова И.В. Цифровая криминалистика: криминалистические инструменты и технологии, применяемые при проведении расследований // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2025. № 2. С. 379.

оперативно-розыскных мероприятий и экспертных исследований. Так в практику расследования постепенно входит применение дронов (БПЛА) применимых для осуществления фотосъемки места происшествия по некоторым видам преступлений, причем отмечается применение не только летательных дронов, но и возможность использования в необходимых ситуациях подводных дронов. Еще одним перспективным направлением является средства трехмерной съемки, используемые, для создания трехмерных панорам и моделей места происшествия, а также применяются в экспертной деятельности.

2) использование ИТ для поиска, обнаружения, изъятия и фиксации криминалистически значимой информации при оперативно-розыскных мероприятиях и ее предварительное исследование при производстве. Качество расследования преступления зависит от его оперативного сопровождения. Использование ИТ в оперативно-розыскной деятельности также будет являться одними из перспективных направлений[1]. Перечисленные выше ИТ, используемые при производстве следственных действий для поиска, обнаружения, изъятия и фиксации следов преступления, применяются в рамках проведения оперативно-розыскных мероприятий с целью поиска, обнаружения и фиксации ориентирующей информации.

Постановление Пленума Верховного Суда РФ от 19.12.2017 № 51 «О практике применения законодательства при рассмотрении уголовных дел в суде первой инстанции (общий порядок судопроизводства)»[2] разъясняет порядок исследования доказательств, представленных в электронном виде. Пленум указывает, что документы, приобщенные к материалам уголовного дела на

---

[1] Воробьев Д.С. Современное использование информационных технологий в раскрытии и расследовании преступлений // Неделя российской науки в Рязанском филиале Московского университета МВД России имени В.Я. Кикотя: сборник научных трудов. Рязань, 2025. С. 403.

[2] О практике применения законодательства при рассмотрении уголовных дел в суде первой инстанции (общий порядок судопроизводства): Постановление Пленума Верховного Суда РФ от 19.12.2017 № 51 [Электронный ресурс]. URL: www.pravo.gov.ru (дата обращения: 12.01.2026).

электронных носителях (компакт-дисках, флеш-картах), подлежат осмотру и исследованию в судебном заседании. Суд должен обеспечить возможность сторонам ознакомиться с содержащейся на них информацией. Если для этого требуются специальные познания или технические средства, суд вправе привлечь специалиста.

3) использование ИТ для регистрации и розыска криминалистически значимых объектов (международного формата – учеты Международной организации уголовной полиции «Интерпол», федерального, регионального (зона обслуживания республики, края, области), местного (зона обслуживания городского и районного (муниципального) уровня):

– автоматизированные статистические, оперативно-справочные, розыскные, криминалистические, экспертно-криминалистические учеты;

– многофункциональные автоматизированные системы, в которых имеется функция регистрации и розыска криминалистически значимых объектов (аппаратно-программный комплекс «Поток»; стационарный аппаратно-программный комплекс автоматического распознавания государственных регистрационных знаков транспортных средств и фиксации нарушений ПДД «АвтоУраган ВСМ2»; аппаратно-программный комплекс «Безопасный город» и др.);

– учеты, которые непосредственно с деятельностью по расследованию и раскрытию преступлений не связаны, т.к. в них отсутствует функция регистрации и розыска криминалистически значимых объектов). Такие автоматизированные информационные поисковые системы (АИПС) используются различными организациями и учреждениями для качественного осуществления своей деятельности.

4) использование ИТ для обеспечения ведомственного и межведомственного взаимодействия правоохранительных органов, а также дистанционного производства следственных действий (допрос, очная ставка, опознание). В 2012 г. была утверждена Концепция создания единой системы информационно-аналитического обеспечения деятельности МВД России

(ИСОД – совокупность используемых в МВД России автоматизированных систем обработки информации, программно-аппаратных комплексов и комплексов программно-технических средств, систем связи и передачи данных, необходимых для эффективного обеспечения деятельности). Реализация данного проекта осуществляется поэтапно, на сегодняшний большая часть работы выполнена[1]. В 2015 г. в рамках исполнения Государственного контракта от 03.12.2013 № 0410/123 Министерством связи и массовых коммуникаций РФ начато создание единой информационно-аналитической системы Следственного комитета РФ (аналог ИСОД МВД России).

Последующее использования ИТ в межведомственном взаимодействии правоохранительных органов обуславливает объединение ведомственных информационно-аналитических систем на единой информационной платформе, так как это диктуется целями и задачами деятельности этих органов, что значительно увеличит качество их работы.

Кроме того, в соответствии со ст. 189.1 УПК РФ (введена Федеральным законом от 30.12.2021 № 501-ФЗ) следователь вправе провести допрос, очную ставку, опознание путем использования систем видео-конференц-связи государственных органов, осуществляющих предварительное расследование, при наличии технической возможности, т.е. допущена возможность дистанционного производства следственных действий, и соответственно применения информационно-телекоммуникационных технологий.

5) использование ИТ в судебно-экспертной деятельности. В судебно-экспертной деятельности ИТ используются уже более 50 лет. Оно осуществляется по следующим направлениям:

– ИТ используемые для автоматизации сбора и обработки экспериментальных данных, получаемых в ходе физико-химических, почвоведческих, биологических и других исследований методами

[1] Распопова П.В. Роль информационного обеспечения и информационных технологий в раскрытии и расследовании преступлений // Актуальные проблемы науки и практики. 2025. № 52. С. 134.

хроматографии, масс-спектрометрии, ультрафиолетовой, инфракрасной спектроскопии, рентгеноспектрального, рентгеноструктурного, атомного спектрального и других видов анализа[1];

– создание банков данных и автоматизированных информационно-поисковых систем (АИПС) по конкретным объектам экспертизы, с использованием ИТ по накоплению, обработке больших массивов информации и выдаче по запросу соответствующих данных;

– ИТ, применяемые анализа изображений при проведении экспертных исследований почерковедческих, дактилоскопических, трасологических, баллистических, портретных для решения идентификационных и диагностических задач;

– использования ИТ при проведении экспертиз (пожарно-технических, взрывотехнических, автотехнических и др.) для выполнения расчетов по формулам для моделирования условий протекания исследуемого явления;

– использование ИТ поддержки принятия решений в судебно-экспертной сфере не только для автоматизации исследования, но и получения экспертного заключения.

Детальные разъяснения содержатся в Постановлении Пленума Верховного Суда РФ от 25.12.2018 № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)»[2]. В нем Пленум, в частности, разъясняет, что понимается под незаконным оборотом специальных технических средств, предназначенных для негласного получения информации. Важным является указание на то, что при рассмотрении дел данной категории

---

[1] Шигапова Л.Р. Применение современных информационных технологий на этапе предварительного расследования // Моя профессиональная карьера. 2023. № 55. С. 209.

[2] О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации): Постановление Пленума Верховного Суда РФ от 25.12.2018 № 46 [Электронный ресурс]. URL: www.pravo.gov.ru (дата обращения: 12.01.2026).

судам необходимо учитывать возможности современных информационных технологий и то, что многие бытовые устройства (например, смартфоны) могут обладать функциями скрытой записи, однако их отнесение к специальным техническим средствам требует заключения эксперта.

Как справедливо отмечают ученые, процессы цифровизации в судебно-экспертной деятельности дали новый импульс развитию направлений использования ИТ – систем искусственного интеллекта (программных комплексов автоматизированного решения экспертных задач).

6) использование ИТ в организации и планировании расследования, организационно-тактическом обеспечении производства следственных действий и в методике расследования отдельных видов и групп преступлений[1]. Следователи получили возможность находить криминалистические рекомендации по расследуемым им убийствам, находя аналогичную следственную ситуацию в справочнике, т.е. практические работники получили фактическое обоснование для принятия решения в виде опыта аналогичного расследования (ИТ поддержки принятия решений). По сути, проводимыми исследованиями было установлено, что основные элементы организации, планирования и методики расследования преступлений можно типизировать и изложить в виде программ и алгоритмов[2].

Развитие информационных технологий и их интеграция в деятельность следователя, а также исследования ученых-криминалистов позволяют сделать шаг от информационно-справочного программного комплекса «Автоматизированное рабочее место следователя» (АРМ «Досудебное производство»), который оптимизировал деятельность следователя по документированию, фиксации информации при расследовании преступлений, к

---

[1] Кравченко Е.В., Пухкалова М.О. Проблемные аспекты применения информационных технологий в расследовании преступлений в цифровом пространстве // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2024. № 2. С. 115.

[2] Долженко Н.И., Подмоков Н.С. Информационные технологии как криминалистические средства расследования и борьбы с преступностью // Тенденции развития науки и образования. 2024. № 6. С. 120.

созданию и активному применению АИС в виде автоматизированных методик расследования отдельных видов преступлений, включающих в себя: актуальную информацию об элементах криминалистической характеристики преступления (типовая компьютерная модель преступления); перечень обстоятельств, подлежащих установлению при расследовании данного вида или группы преступлений; типичные следственные ситуации первоначального этапа расследования; типовые следственные версии; алгоритмы следственных, проверочных, организационно-подготовительных, процессуальных и иных действий, производимых в конкретных следственных ситуациях для их разрешения и др.) и представляющих из себя автоматизированные информационные системы поддержки принятия следователем решений: по организации и планированию расследования в целом, а также следственных действий и тактических операций, производимых в рамках данного расследования; по тактике производства следственных действий; методике расследования. Данные АИС могут реализовываться на базе стационарных аппаратно-программных комплексов, а также на смартфонах в виде приложения[1].

Таким образом, основными направлениями использования ИТ в расследовании и раскрытии преступлений являются:

- использование ИТ для поиска, обнаружения, изъятия и фиксации криминалистически значимой информации при производстве следственных действий и ее предварительное исследование;

- использование ИТ для поиска, обнаружения, изъятия и фиксации криминалистически значимой информации оперативно-розыскных мероприятий и ее предварительное исследование при производстве;

- использование ИТ для регистрации и розыска криминалистически значимых объектов (автоматизированные статистические, оперативно-

[1] Соломатина А.Г. Использование информационных технологий при расследовании преступлений // Уголовное судопроизводство России и зарубежных государств: проблемы и перспективы развития: сборник научных трудов. Санкт-Петербург, 2023. С. 305.

справочные, розыскные, криминалистические, экспертно-криминалистические учеты; многофункциональные автоматизированные системы, в которых имеется функция регистрации и розыска криминалистически значимых объектов; учеты, которые непосредственно с деятельностью по расследованию и раскрытию преступлений не связаны, т.к. в них отсутствует функция регистрации и розыска криминалистически значимых объектов);

- использование ИТ для обеспечения ведомственного и межведомственного взаимодействия правоохранительных органов, а также дистанционного производства следственных действий (допрос, очная ставка, опознание);

- использование ИТ в судебно-экспертной деятельности;

- использование ИТ в организации и планировании расследования, организационно-тактическом обеспечении производства следственных действий и в методике расследования отдельных видов и групп преступлений.

Стадия возбуждения уголовного дела, будучи исходным моментом процессуальной деятельности, характеризуется необходимостью быстрого и точного анализа первичной информации для принятия обоснованного решения. Роль ИКТ на данном этапе трудно переоценить.

Первостепенное значение приобретают информационно-справочные и учетные системы. При поступлении сообщения о преступлении следователь или дознаватель обязан проверить фигурирующих в нем лиц, предметы, транспортные средства по соответствующим криминалистическим и оперативно-розыскным учетам. Автоматизированные запросы в базы данных МВД, ФНС, ФССП, Росреестр позволяют в кратчайшие сроки установить криминальную историю личности, данные о собственности, возможную причастность к другим правонарушениям, что способствует правильной квалификации события и оценке его достоверности. Геоинформационные системы помогают анализировать место предполагаемого преступления, его инфраструктуру, пути подъезда и отъезда, что может быть использовано как при проверке, так и позднее – при планировании первоначальных следственных

действий[1].

Средства коммуникации, в особенности электронная почта с усиленной квалифицированной подписью и системы межведомственного электронного взаимодействия (СМЭВ), позволяют оперативно направлять и получать ответы на официальные запросы в государственные органы и учреждения, что значительно сокращает сроки проведения проверки, регламентированные статьей 144 УПК РФ. Важным инструментом становится также программное обеспечение для первичного анализа цифровых носителей, поступающих с заявлением о преступлении (например, флеш-карт с компрометирующими материалами). Специализированные программы позволяют создать криминалистическую копию носителя без риска повреждения оригинальных данных, провести предварительный анализ файловой структуры и метаданных, что может предоставить основания для возбуждения дела.

Современные поправки в законодательство, допускающие дистанционный формат приема сообщений о преступлении (через официальные интернет-приемные), также требуют применения соответствующих ИКТ для верификации заявителя, обеспечения конфиденциальности и юридической силы такого обращения.

Этап предварительного расследования представляет собой наиболее насыщенную и сложную фазу, где ИКТ применяются максимально широко и разнообразно, пронизывая все направления работы.

На стадии планирования и выдвижения версий на первый план выходят аналитические технологии. Программные комплексы для анализа больших данных помогают обрабатывать массивы информации из банковских выписок, журналов звонков (CDR), записей с камер видеонаблюдения, данных с GPS-трекеров. Алгоритмы машинного обучения способны выявлять аномалии, кластеризировать события, строить вероятностные модели развития ситуации.

---

[1] Казанцев С.Я,, Романова Г.В. К вопросу об использовании информационно-поисковых технологий в работе следователя // Криминологический журнал. 2025. № 3. С. 74.

Инструменты визуализации (например, программы для создания интеллект-карт и временных шкал) помогают следователю структурировать гипотезы, наглядно представлять логические связи между эпизодами и лицами[1].

Собирание доказательств сегодня немыслимо без целого арсенала специализированных ИКТ. При производстве следственных действий активно используются:

- аудиовизуальные средства фиксации: цифровые фото- и видеокамеры высокого разрешения, обеспечивающие детальную съемку места происшествия, вещественных доказательств. Современные технологии панорамной (360°) съемки и 3D-сканирования позволяют создать точную и интерактивную виртуальную модель места происшествия, к которой можно неоднократно возвращаться в ходе расследования и в суде;

- средства видеоконференцсвязи: на основании статей 278.1 и 189 УПК РФ дистанционный допрос свидетелей, потерпевших, экспертов, находящихся в другом городе или стране, становится рутинной практикой. Подобный подход экономит время и ресурсы, а применение систем с криптографической защитой канала гарантирует сохранность передаваемой информации;

- электронный документооборот: формирование процессуальных документов в электронном виде с использованием усиленной квалифицированной электронной подписи упрощает их согласование, подписание и передачу, в том числе в суд для санкционирования процессуальных действий. Системы сквозного шифрования защищают конфиденциальность материалов дела;

- цифровая криминалистика, которая включает изъятие и исследование электронных носителей – обязательный элемент расследования большинства категорий дел. Аппаратно-программные комплексы позволяют производить «захват» данных с жестких дисков, смартфонов, облачных хранилищ,

[1] Тайтубаева Л.М. Понятие информационных технологий и их значение при использовании в ходе расследования преступлений // Право и управление. 2025. № 6. С. 238.

осуществлять поиск по ключевым словам, восстанавливать удаленные файлы, анализировать историю действий пользователя в сети, устанавливать связи между устройствами. При расследовании экономических преступлений применяется программное обеспечение для аудита финансовых данных и выявления подозрительных транзакций[1].

В процессе проверки и оценки доказательств используются экспертные системы и базы знаний, которые могут оказывать консультативную поддержку следователю при оценке типичных признаков подделки документов, определении вида наркотического вещества по фотографии и прочем. Технологии сравнения цифровых голосовых отпечатков или почерка также находят свое применение, хотя их результаты зачастую носят ориентировочный характер и требуют традиционной экспертизы.

Организационно-управленческие ИКТ, такие как АРМ следователя и системы процессуального контроля, интегрируют все перечисленные функции, обеспечивая единое рабочее пространство, напоминание о процессуальных сроках, контроль поручений и ведение электронного журнала учета производства.

На судебных стадиях уголовного процесса доминирующей функцией ИКТ становится наглядное и убедительное представление собранных доказательств суду и участникам процесса. Технологии трансформируются из инструмента поиска в инструмент доказывания.

Здесь широко применяются системы мультимедийной презентации. Вместо традиционных томов бумажных материалов сторона обвинения и защиты могут использовать интерактивные стенды, на которых в реальном времени демонстрируются оцифрованные документы, фотографии, схемы, видеофрагменты. Виртуальные 3D-реконструкции места преступления позволяют судье и присяжным заседателям «погрузиться» в обстановку

---

[1] Калюжный А.Н. Векторы реализации потенциала информационных технологий в деятельности оперативных и следственных подразделений // Вестник Восточно-Сибирского института МВД России. 2025. № 2. С. 141.

события, самостоятельно рассмотреть детали с разных ракурсов, что существенно повышает восприятие и понимание обстоятельств дела.

Технологии ВКС, помимо допроса удаленных свидетелей, активно используются для проведения судебных заседаний в режиме онлайн по определенным категориям дел или при наличии ходатайств участников процесса, что закреплено в статье 241.1 УПК РФ. Подобная практика повышает доступность правосудия и экономит средства[1].

Экспертные заключения, подготовленные с использованием сложного программного обеспечения для криминалистического анализа данных, могут быть представлены в интерактивной форме. Эксперт имеет возможность непосредственно в зале судебного заседания продемонстрировать ход своего исследования, например, показать, каким образом были восстановлены удаленные сообщения или установлен маршрут перемещения автомобиля по данным спутниковой навигации. Кроме того, системы электронного судопроизводства, внедряемые в рамках создания «электронного правосудия», обеспечивают подачу ходатайств, ознакомление с материалами дела и получение судебных актов в цифровом формате, что делает судебный процесс более прозрачным и эффективным[2].

Использование информационно-коммуникационных технологий в практической деятельности Отдела МВД России по Белебеевскому району в настоящее время характеризуется наличием базового уровня оснащения при существенном недоиспользовании имеющегося потенциала цифровых средств в технико-криминалистическом обеспечении расследования преступлений.

В Отделе МВД России по Белебеевскому району работает достаточно сбалансированный по опыту коллектив следственных работников, где

---

[1] Рахмонбердиев Б.Б. Применение информационных технологий в органах предварительного расследования // Уголовное судопроизводство России и зарубежных государств: проблемы и перспективы развития: сборник научных трудов. Санкт-Петербург, 2023. С. 661.

[2] Суетина П.А. Использование информационно-коммуникационных технологий в расследовании преступлений // Современные достижения молодых исследователей: сборник научных трудов. Пенза, 2023. С. 91.

примерно четверть составляют молодые специалисты со стажем до трех лет, около сорока процентов сотрудников имеют стаж от трех до десяти лет и треть относится к числу наиболее опытных работников со стажем более десяти лет. Такое распределение создает предпосылки для сочетания свежего взгляда на возможности технологий у начинающих следователей и глубокого понимания криминалистических процессов у опытных кадров. Однако на практике синергия этих групп реализуется недостаточно эффективно из-за отсутствия системного наставничества и обмена опытом в сфере применения цифровых инструментов.

Интенсивное внедрение ИКТ в уголовный процесс порождает ряд серьезных правовых и этических проблем, требующих внимательного осмысления и законодательного регулирования.

Во-первых, существует проблема допустимости доказательств, полученных с помощью новых технологий. Российское законодательство, в целом, идет по пути признания таких доказательств при условии соблюдения процедуры их получения и фиксации. Однако остаются вопросы, связанные с применением технологий, носящих скрытый или инвазивный характер (например, глубокий анализ данных из социальных сетей, технологии распознавания лиц в публичных пространствах). Необходим четкий баланс между интересами следствия и правом граждан на неприкосновенность частной жизни (статья 23 Конституции РФ).

Во-вторых, актуален вопрос обеспечения равноправия сторон. Доступ к передовым криминалистическим ИКТ зачастую ограничен государственными правоохранительными органами. Защита может оказаться в заведомо невыгодном положении, не имея финансовых или технических возможностей для проведения собственного независимого цифрового исследования. Гарантирование права на защиту в цифровую эпоху требует развития института судебных экспертов, работающих в интересах защиты, и возможного предоставления им доступа к нейтральным инструментам анализа.

В-третьих, сложной задачей является верификация и сохранность

цифровых доказательств. Цифровые данные легко изменяемы и уязвимы для повреждения. Процессуальный закон и криминалистическая методика должны строго регламентировать применение криптографических хэш-сумм (контрольных сумм) для обеспечения целостности изъятых электронных носителей, использование сертифицированного программного обеспечения для создания криминалистических копий и обеспечение надлежащих условий хранения цифровых доказательств.

В-четвертых, эффективное использование ИКТ требует от следователей, дознавателей, прокуроров, судей и адвокатов постоянного повышения цифровой грамотности. Отсутствие необходимых компетенций может привести как к ошибкам при изъятии доказательств, так и к их неправильной оценке в суде.

В-пятых, существуют этические границы использования технологий. Применение прогнозной аналитики для оценки вероятности рецидива или «профайлинга» потенциальных преступников, хотя и является перспективным направлением, таит в себе угрозу дискриминации и предвзятого отношения, основанного не на конкретных деяниях, а на статистических алгоритмах.

Таким образом, проведенный анализ позволяет утверждать, что информационно-коммуникационные технологии стали системообразующим элементом современного уголовного судопроизводства, качественно изменяющим его ландшафт. Их классификация по функциональному признаку – на информационно-аналитические, коммуникационные, криминалистические и организационно-управленческие – наиболее релевантна для следственной практики, позволяя гибко подбирать инструментарий под конкретные задачи каждого этапа расследования: от первичной проверки сообщения о преступлении до судебного разбирательства.

§ 2. Актуальные проблемы и перспективы развития использования информационно-коммуникационных технологий в технико-криминалистическом обеспечении

Проблемы и перспективы развития использования информационно-коммуникационных технологий в технико-криминалистическом обеспечении представляют собой сложный и динамичный предмет научного и практического осмысления, находящийся на стыке юриспруденции, криминалистики и компьютерных наук. Глубина и масштаб данной темы обусловлены тем фундаментальным влиянием, которое цифровая трансформация оказывает на природу преступной деятельности и, как следствие, на систему противодействия ей.

Технико-криминалистическое обеспечение, исторически сформировавшееся как арсенал методов и средств работы с материальными следами в физическом мире, сегодня переживает период болезненной, но необходимой адаптации к реалиям гибридной среды, где электронные отпечатки преступления зачастую обладают большей доказательственной ценностью, чем их вещественные аналоги. Однако стремительное внедрение информационно-коммуникационных технологий в следственную и экспертно-криминалистическую практику происходит неравномерно и сталкивается с целым комплексом системных противоречий, разрешение которых определит облик правоохранительной системы на десятилетия вперед[1].

Российский законодатель, осознавая вызовы времени, вносит постоянные коррективы в нормативную базу, примером чему служат изменения в Уголовно-процессуальный кодекс, легализующие дистанционный формат следственных действий, электронный документооборот и определенные формы цифровых доказательств. Но само по себе право, будучи по природе

[1] Таашев Д.Б. Проблемные аспекты применения информационных технологий в расследовании преступлений в цифровом пространстве // Российский научный вестник. 2025. № 4. С. 254.

консервативным, не способно мгновенно реагировать на каждый технологический прорыв, в связи с чем между передовыми возможностями техники и их легальным, методически выверенным применением возникает опасный разрыв, требующий скорейшего преодоления.

Одной из наиболее острых проблем, непосредственно затрагивающих самую суть уголовного судопроизводства, выступает вопрос процессуальной легитимности и доказательственной силы данных, полученных с применением новейших информационно-коммуникационных средств.

Современное технико-криминалистическое обеспечение уже немыслимо без сложных аппаратно-программных комплексов для изъятия и анализа данных с электронных носителей, инструментов криптографии для защиты каналов связи, систем искусственного интеллекта, применяемых для распознавания образов, голоса, почерка или выявления скрытых закономерностей в массивах информации. Однако процедурные аспекты использования подобных технологий зачастую остаются вне детальной правовой регламентации[1].

Действующие нормы УПК РФ, даже с учетом последних поправок, задают лишь самые общие рамки, оставляя на усмотрение следственной и судебной практики решение таких принципиальных вопросов, как критерии допустимости алгоритмов машинного обучения в качестве инструмента экспертного исследования, стандарты верификации и сертификации используемого программного обеспечения, порядок документального оформления действий, совершаемых автоматизированными системами. Например, применение технологии блокчейн для обеспечения неизменности цепочки доказательств или использование нейросетей для прогнозного моделирования поведения подозреваемого требует разработки специальных процессуальных протоколов, которые гарантировали бы проверяемость, повторяемость и понятность полученных результатов для всех участников

[1] Ардавов М.М. О проблемных аспектах применения информационных технологий в расследовании преступлений // Право и управление. 2025. № 7. С. 133.

процесса.

Отсутствие подобных протоколов создает почву для многочисленных споров в суде, ставит под сомнение результаты расследования и, в конечном счете, подрывает доверие к системе правосудия. Более того, возникает проблема «цифрового двойника» расследования, когда собранные электронные доказательства, будучи по своей природе легко копируемыми и трансформируемыми, должны сохранять аутентичность и целостность на протяжении всего производства по делу.

Недостаточно развитая нормативная база, регламентирующая применение криптографических хэш-сумм, электронных подписей и защищенных носителей для хранения вещественных доказательств в цифровой форме, порождает риски утраты или фальсификации улик.

Второй пласт трудностей связан с нарастающим технологическим дисбалансом между возможностями правоохранительных органов и современными криминальными структурами. Преступные сообщества, обладая значительными финансовыми ресурсами и не будучи скованными бюрократическими процедурами, демонстрируют поразительную гибкость и скорость в освоении новейших технологий[1].

Активное использование криптовалют и миксеров для отмывания средств, эксплуатация анонимных сетей и зашифрованных мессенджеров для коммуникации, применение сложных фишинговых атак и вредоносного программного обеспечения, создание дипфейков для манипуляции общественным мнением или шантажа – все это реалии сегодняшнего дня. Государственные же правоохранительные органы, особенно на региональном уровне, нередко сталкиваются с длительным циклом бюджетного планирования, устаревшими процедурами закупок, которые не успевают за жизненным циклом IT-продуктов, и хроническим дефицитом квалифицированных кадров. Результатом становится ситуация, при которой

[1] Губарева А.С. Перспективы и риски использования информационных технологий при расследовании преступлений // Научный альманах. 2025. № 6. С. 73.

технико-криминалистическое обеспечение расследования по многим параметрам отстает от технологического уровня самого преступления.

Попытки догнать ускользающую цифровую реальность за счет единичных закупок дорогостоящего оборудования без построения целостной экосистемы (включающей регулярное обновление, техподдержку и обучение) оказываются малоэффективными. Преодоление данного разрыва требует не просто увеличения финансирования, но и пересмотра самой философии технического оснащения, перехода к модели гибкого, проектного внедрения технологий, возможно, через механизмы государственно-частного партнерства, привлечения ресурсов научно-исследовательских институтов и создания межведомственных центров коллективного пользования уникальным и дорогостоящим оборудованием.

Методическая неразвитость представляет собой не менее серьезное препятствие на пути интеграции информационно-коммуникационных технологий в повседневную следственную практику. Существующие методики технико-криминалистического обеспечения в значительной степени ориентированы на работу с традиционными, материальными следами: отпечатками пальцев, следами обуви, микрочастицами, холодным и огнестрельным оружием[1].

Появление цифровой среды диктует необходимость разработки и законодательного закрепления принципиально новых алгоритмов действий. Так, осмотр места происшествия в современном понимании должен включать не только фиксацию физической обстановки, но и процедуру выявления всех потенциальных источников цифровой информации – от смартфонов, ноутбуков и планшетов до серверного оборудования, систем «умного дома», автомобильных регистраторов и носимых гаджетов. Каждый из таких источников требует специфического подхода к изъятию, упаковке и

[1] Воробьев Д.С. Современное использование информационных технологий в раскрытии и расследовании преступлений // Неделя российской науки в Рязанском филиале Московского университета МВД России имени В.Я. Кикотя: сборник научных трудов. Рязань, 2025. С. 404.

транспортировке, исключающего повреждение данных или их случайное изменение.

Отсутствие единых, обязательных для всех правоохранительных органов методических рекомендаций, охватывающих полный жизненный цикл цифрового доказательства, ведет к разнобою в практике, ошибкам на критически важной начальной стадии, что делает невозможным последующее использование полученных сведений в суде.

Кроме того, стремительно эволюционируют и сами формы криминальных посягательств, опережая разработку адекватных средств противодействия. Преступления в сфере децентрализованных финансов, манипуляции с искусственным интеллектом, использование возможностей метавселенных для совершения противоправных действий – все эти явления требуют опережающих научных исследований и создания специализированных инструментариев в рамках технико-криминалистического обеспечения, что сегодня осуществляется явно недостаточными темпами.

Кадровый кризис, усугубляемый цифровым переходом, является, пожалуй, наиболее чувствительной и труднорешаемой проблемой. Эффективное применение сложного информационно-коммуникационного инструментария предполагает не просто базовую компьютерную грамотность, а наличие у следователей, дознавателей, экспертов-криминалистов и судей глубоких, постоянно обновляемых знаний в конкретных технологических областях[1].

Действующая система профессиональной подготовки и повышения квалификации в силовых ведомствах зачастую носит формальный характер, отстает от технологических трендов и не обеспечивает формирование практических навыков работы с новейшим оборудованием и программным обеспечением. Как следствие, дорогостоящие технические средства простаивают или используются в минимальном, далеко не полном

[1] Архипова П.С. Отдельные проблемы использования информационных технологий в расследовании преступлений // Студенческий вестник. 2024. № 11. С. 21.

функциональном объеме. Особенно остро ощущается дефицит экспертов в области цифровой криминалистики, способных не только нажимать кнопки в интерфейсе готовой программы, но и понимать архитектуру современных операционных систем, принципы работы сетевых протоколов, основы криптографии и машинного обучения. Без таких специалистов невозможно критически оценить достоверность выводов, сгенерированных автоматизированной системой, или провести независимое исследование в интересах защиты.

Для изучения эффективности использования информационно-коммуникационных технологий в практике технико-криминалистического обеспечения расследования преступлений ОМВД России по Белебеевскому району был проведен опрос (анкетный лист дан в приложении). В исследовании участвовали 33 сотрудника (5 участковых уполномоченных полиции, 8 оперативных сотрудника, 10 следователей и 10 дознавателей).

Распределение респондентов по стажу работы оказалось следующим: 8 человек, или 24,2% от общего числа опрошенных, имели стаж до 3 лет; 14 человек, или 42,4%, обладали стажем от 3 до 10 лет; и 11 человек, или 33,3%, проработали в следственных подразделениях более 10 лет. Такое распределение обеспечило репрезентативность выборки, позволив учесть мнения как молодых специалистов, активно осваивающих современные технологии, так и опытных сотрудников, способных сравнивать новые методы работы с традиционными подходами. Анализ ответов позволил составить детальную картину восприятия роли информационно-коммуникационных технологий, их реального использования в повседневной практике, а также выявить системные проблемы, препятствующие более полному внедрению цифровых инструментов в деятельность следователя.

Первый вопрос анкеты был направлен на выявление общей оценки значимости информационно-коммуникационных технологий для успешного расследования преступлений. Полученные данные свидетельствуют о практически единодушном признании важности технологий в современной

следственной работе. Крайне высокую значимость, подразумевающую невозможность расследования без использования ИКТ, отметили 12 респондентов, что составило 36,4% от общего числа опрошенных. Высокую значимость, характеризующую технологии как существенно помогающий инструмент, указали 17 человек, или 51,5%. Таким образом, в совокупности 29 человек, или 87,9%, оценивают роль ИКТ как высокую или крайне высокую. Умеренную значимость, рассматривая технологии как полезное дополнение к традиционным методам, отметили 4 человека, или 12,1%. Никто из опрошенных не выбрал вариант, оценивающий значимость технологий как незначительную и отдающий предпочтение традиционным методам. Полученные цифры убедительно демонстрируют, что современные следователи осознают необратимость цифровизации и необходимость использования технологического инструментария для эффективного противодействия преступности.

Ответы на второй вопрос, касающийся регулярности использования различных видов информационно-коммуникационных технологий, позволили выявить реальную картину применения цифровых инструментов в повседневной практике. Наиболее востребованными оказались мобильные устройства и приложения для выезда на место происшествия, которые регулярно используют 27 респондентов, что составляет 81,8%. Системы видеоконференцсвязи для взаимодействия с другими органами и судами также широко применяются, их использование подтвердили 24 человека, или 72,7%. Специализированные программные комплексы для составления схем, фотосъемки и работы с базами данных используются 21 респондентом, или 63,6%. Средства криптографической защиты служебной информации применяют 15 человек, или 45,5%. Аппаратно-программные комплексы для изъятия и предварительного анализа данных с электронных носителей используются реже, их регулярное применение отметили 12 респондентов, или 36,4%. Два человека, или 6,1%, указали иные технологии, не вошедшие в перечень, в частности, использование геоинформационных систем и сервисов

аналитики открытых данных. Примечательно, что базовые и коммуникационные технологии используются значительно чаще, чем сложные криминалистические комплексы, что свидетельствует о неравномерности технологического развития различных направлений следственной деятельности.

Третий вопрос был посвящен целям, с которыми следователи используют информационно-коммуникационные технологии наиболее часто, при этом респонденты могли выбрать не более двух основных вариантов. Наиболее популярной целью оказался поиск и проверка информации в оперативно-справочных и розыскных учетах, этот вариант выбрали 28 человек, или 84,8%. На втором месте по частоте упоминаний оказалось документирование хода и результатов следственных действий, эту цель указали 22 респондента, или 66,7%. Коммуникация и оперативный обмен информацией с другими участниками процесса являются важной целью для 18 человек, или 54,5%. Фиксация обстановки места происшествия с использованием современных средств, таких как 3D-сканирование или панорамная съемка, отмечена 10 респондентами, или 30,3%. Анализ больших массивов данных, например финансовых транзакций или соединений абонентов, назвали важной целью 8 человек, или 24,2%. Экспертная деятельность и взаимодействие с экспертно-криминалистическими подразделениями оказались приоритетом для 6 респондентов, или 18,2%.

Полученное распределение показывает, что в настоящее время технологии воспринимаются следователями преимущественно как инструмент для решения традиционных, рутинных задач, тогда как их аналитический и экспертный потенциал используется далеко не в полной мере.

Четвертый вопрос оценивал уровень технической оснащенности подразделений с точки зрения самих сотрудников. Полностью соответствующим современным задачам сочли оснащение лишь 4 человека, или 12,1% опрошенных. Большинство респондентов, а именно 19 человек или 57,6%, указали, что оснащение в основном соответствует требованиям, но при

этом отметили наличие отдельных недостатков. Частичное соответствие с необходимостью существенного обновления констатировали 8 человек, или 24,2%. Двое опрошенных, или 6,1%, оценили оснащение как практически не соответствующее современным требованиям. Таким образом, в совокупности 29 человек, или 87,9%, так или иначе фиксируют наличие проблем с техническим оснащением, что является тревожным сигналом и указывает на необходимость системного обновления материально-технической базы следственных подразделений.

Пятый вопрос касался самооценки сотрудниками уровня своей подготовки для эффективного использования имеющихся информационно-коммуникационных технологий. Полностью достаточным свой уровень сочли 10 человек, или 30,3%. Наиболее многочисленная группа, 17 респондентов или 51,5%, указала, что в целом знаний и навыков хватает, однако по некоторым новым технологиям требуется дополнительное обучение. Затруднились с ответом 2 человека, или 6,1%. Четверо опрошенных, или 12,1%, признали наличие значительного дефицита знаний и фрагментарный характер навыков. Полученные данные свидетельствуют о существовании серьезного разрыва между наличием технологий и готовностью кадров к их полноценному использованию, при этом более половины респондентов осознают потребность в дополнительном обучении, что формирует запрос на развитие системы профессиональной подготовки и повышения квалификации.

Шестой вопрос был направлен на выявление частоты возникновения технических проблем, затрудняющих использование информационно-коммуникационных технологий. Ежедневно или несколько раз в неделю сталкиваются с такими проблемами 7 человек, или 21,2%. Несколько раз в месяц проблемы возникают у 13 респондентов, или 39,4%. Достаточно редко, раз в несколько месяцев, с трудностями сталкиваются 9 человек, или 27,3%. Практически никогда не испытывают технических проблем лишь 4 человека, или 12,1%. Суммируя первые две группы, получаем, что 20 человек, или 60,6% опрошенных, сталкиваются с техническими неполадками с

периодичностью не реже нескольких раз в месяц, что существенно снижает эффективность использования технологий и формирует негативное отношение к их надежности.

Седьмой вопрос оценивал влияние использования информационно-коммуникационных технологий на временные затраты при выполнении процессуальных действий. Существенное сокращение времени, более чем на 30%, отметили 9 человек, или 27,3%. Умеренное сокращение, примерно на 10-30 процентов, указали 19 респондентов, или 57,6%. Отсутствие значительного влияния на сроки констатировали 3 человека, или 9,1%. Двое опрошенных, или 6,1%, отметили, что использование технологий иногда даже увеличивает временные затраты из-за сложности работы с ними. Таким образом, подавляющее большинство, 28 человек или 84,9%, все же фиксируют положительный эффект от внедрения технологий в виде экономии времени, однако степень этой экономии варьируется.

Восьмой вопрос затрагивал принципиально важную проблему влияния информационно-коммуникационных технологий на объективность и непредвзятость доказательственной базы. Значительное положительное влияние, обусловленное полнотой и неизбирательностью фиксации информации, отметили 15 человек, или 45,5%. Скорее положительное влияние, но с оговоркой о необходимости строгого процессуального контроля, указали 13 респондентов, или 39,4%. Затруднились с ответом 3 человека, или 9,1%. Двое опрошенных, или 6,1%, высказали мнение, что традиционные протоколы и вещественные доказательства надежнее цифровых. Суммируя первые две группы, получаем, что 28 человек, или 84,9%, в той или иной степени признают позитивный вклад технологий в повышение объективности доказательственной базы, что является важным аргументом в пользу дальнейшего внедрения цифровых средств фиксации.

Девятый вопрос был посвящен проблеме противодействия использованию информационно-коммуникационных технологий со стороны лиц, причастных к преступной деятельности. Как постоянную и серьезную

проблему это оценили 7 человек, или 21,2%. Периодически сталкиваются с таким противодействием 16 респондентов, или 48,5%. Редко встречаются с подобными ситуациями 8 человек, или 24,2%. Не сталкивались с противодействием лишь 2 человека, или 6,1%. Совокупность первых двух групп показывает, что 23 человека, или 69,7% опрошенных, регулярно сталкиваются с попытками преступников использовать шифрование, уничтожать цифровые следы или иным образом противодействовать расследованию с использованием технологий, что подтверждает наличие технологической гонки между правоохранительными органами и криминальной средой.

Десятый вопрос носил прогностический характер и предлагал респондентам оценить, какие направления развития информационно-коммуникационных технологий будут наиболее востребованы в следственной практике в ближайшие 3-5 лет, с возможностью выбора нескольких вариантов. Наибольшее число голосов, 28 человек или 84,8%, получило направление, связанное с искусственным интеллектом для анализа данных и выявления связей. Развитие средств анализа информации из открытых источников поддержали 24 человека, или 72,7%. Расширенное использование биометрических технологий отметили 20 респондентов, или 60,6%. Развитие облачных платформ для межведомственного взаимодействия указали 19 человек, или 57,6%. Автоматизацию рутинных процессов документооборота выбрали 17 человек, или 51,5%. Прогнозную аналитику и моделирование криминальных ситуаций поддержали 15 респондентов, или 45,5%. Полученные данные демонстрируют высокий запрос практиков на внедрение интеллектуальных систем, способных обрабатывать большие объемы информации и выявлять скрытые закономерности.

Одиннадцатый вопрос выявлял мнение респондентов о главных препятствиях для более широкого и эффективного внедрения информационно-коммуникационных технологий, при этом можно было выбрать не более двух вариантов. Наиболее часто называемым препятствием оказалось

недостаточное финансирование и устаревшая материально-техническая база, этот вариант выбрали 26 человек, или 78,8%. На втором месте оказался дефицит специальных знаний и навыков у сотрудников, его отметили 21 человек, или 63,6%. Проблемы информационной безопасности и защиты данных волнуют 14 респондентов, или 42,4%. Несовершенство законодательной базы, регулирующей использование цифровых доказательств, указали 12 человек, или 36,4%. Излишне бюрократизированные процедуры внедрения новых решений отметили 10 респондентов, или 30,3%. Консерватизм и неготовность к изменениям в организации работы назвали 6 человек, или 18,2%. Полученные цифры четко указывают на две главные системные проблемы: недостаток финансирования и кадровый дефицит в части компетенций, решение которых должно стать приоритетным для руководства.

Двенадцатый вопрос фиксировал распределение респондентов по стажу работы, что уже было отражено в начале анализа. Данные о стаже позволяют дифференцировать ответы и выявлять зависимость оценок от профессионального опыта. Анализ в разрезе стажа показывает, что молодые сотрудники со стажем до 3 лет более оптимистично оценивают перспективы внедрения новых технологий, но при этом чаще указывают на недостаток собственных знаний. Сотрудники со стажем от 3 до 10 лет демонстрируют наиболее сбалансированный подход, сочетая понимание технологических возможностей с критической оценкой существующих проблем. Опытные сотрудники со стажем более 10 лет более консервативны в оценках, чаще скептически относятся к полной замене традиционных методов и острее ощущают проблемы, связанные с устаревшей материальной базой.

Подводя общий итог, следует отметить, что проведенное анкетирование позволило получить репрезентативные данные, отражающие реальное состояние дел с внедрением информационно-коммуникационных технологий в следственную практику. Высокий уровень признания значимости технологий, отмеченный 87,9 процента респондентов, сочетается с

критической оценкой материально-технической базы, которую лишь 12,1% считают полностью соответствующей задачам. Существенным барьером выступает дефицит компетенций, который прямо или косвенно признают 69,7% опрошенных. При этом 69,7% регулярно сталкиваются с противодействием со стороны преступников, использующих технологические средства, что создает необходимость опережающего развития правоохранительных технологий. Запрос практиков на внедрение искусственного интеллекта, средств анализа открытых данных и биометрических технологий формирует четкий вектор для определения приоритетов дальнейшего развития информационно-коммуникационного обеспечения следственной деятельности.

Решение кадровой проблемы требует системных инвестиций: интеграции образовательных программ ведущих технических и юридических вузов с запросами правоохранительных органов, создания центров превосходства и стажировок на базе передовых экспертных учреждений, разработки специальных карьерных траекторий и систем материального стимулирования для IT-специалистов, приходящих работать в правоохранительную систему. Без притока свежих умов и кардинального обновления подхода к обучению технологическое переоснащение останется пустой тратой бюджетных средств.

Сопутствующей и крайне важной темой являются этические и социальные дилеммы, порождаемые всепроникающим использованием информационно-коммуникационных технологий в сфере уголовного преследования[1].

Массовое внедрение систем распознавания лиц в публичных пространствах, тотальный сбор и анализ телеметрических данных с мобильных устройств, применение алгоритмов профайлинга для выявления «потенциально опасных» лиц на основе анализа больших данных формируют инфраструктуру тотального наблюдения. Подобные практики, потенциально повышая

[1] Селютин Д.М. Методология использования информационных технологий в расследовании преступлений // Молодой ученый. 2025. № 3. С. 19.

оперативность раскрытия преступлений, несут в себе фундаментальную угрозу приватности, свободе передвижения и ассоциаций, устанавливают de facto презумпцию виновности для граждан, попавших в поле зрения «цифрового ока» государства.

В российском правовом поле вопрос о балансе между безопасностью и свободой требует особенно вдумчивого регулирования. Необходима разработка и принятие четких законодательных гарантий, устанавливающих исчерпывающий перечень оснований и процедур для применения технологий массового наблюдения и прогнозной аналитики, обеспечивающих прозрачность и подконтрольность алгоритмов, принимающих решения, влияющие на права и свободы человека.

Должны быть созданы эффективные механизмы судебного и общественного контроля за деятельностью, связанной с обработкой персональных данных в правоохранительных целях. Игнорирование этих этических соображений чревато не только нарушениями прав конкретных граждан, но и постепенной деградацией доверительных отношений между обществом и государством, что в долгосрочной перспективе подрывает саму легитимность правоохранительной деятельности[1].

Несмотря на масштаб перечисленных проблем, перспективы развития использования информационно-коммуникационных технологий в технико-криминалистическом обеспечении остаются значительными и многообещающими. Основной вектор эволюции видится в движении от разрозненных инструментов к созданию целостной, сквозной цифровой экосистемы поддержки расследования. Ее концептуальным ядром могла бы стать национальная платформа, обеспечивающая безопасную интеграцию существующих ведомственных баз данных (криминалистических, оперативно-розыскных, миграционных, финансовых), систем видеоаналитики,

[1] Долженко Н.И., Подмоков Н.С. Информационные технологии как криминалистические средства расследования и борьбы с преступностью // Тенденции развития науки и образования. 2024. № 6. С. 121.

инструментов цифровой криминалистики и модулей на основе искусственного интеллекта. Подобная платформа предоставила бы следователю, действующему в рамках строго разграниченных прав доступа, единую точку входа для работы с информацией, автоматизируя рутинные задачи по сопоставлению данных, выявлению противоречий, построению графических моделей связей между фигурантами и событиями.

Существенный потенциал заложен в развитии технологий, позволяющих работать с качественно новыми видами цифровых следов, такими как данные с устройств интернета вещей, которые могут фиксировать обстановку в момент преступления, или информация из распределенных реестров (блокчейн), способная обеспечить бесспорное подтверждение тех или иных фактов. Дальнейшее совершенствование средств криптографической защиты открывает путь для повсеместного внедрения полноценного электронного уголовного дела, где каждый процессуальный документ, каждый протокол следственного действия, каждый вывод эксперта существуют в юридически значимом цифровом виде, защищенном от изменений и обеспечивающем прозрачность процедуры ознакомления для защиты[1].

Таким образом, современный этап развития технико-криминалистического обеспечения характеризуется сложным переплетением беспрецедентных технологических возможностей и глубоких системных вызовов. Успешная интеграция информационно-коммуникационных технологий в практику раскрытия и расследования преступлений не может быть сведена к простой закупке оборудования. Она требует комплексного, скоординированного подхода, включающего опережающее развитие процессуального законодательства, создание гибких механизмов финансирования и внедрения инноваций, фундаментальную перестройку системы подготовки и переподготовки кадров, а также проведение

[1] Соломатина А.Г. Использование информационных технологий при расследовании преступлений // Уголовное судопроизводство России и зарубежных государств: проблемы и перспективы развития: сборник научных трудов. Санкт-Петербург, 2023. С. 308.

ответственной общественной дискуссии о допустимых границах технологического вмешательства в частную жизнь.

Перспектива заключается не в том, чтобы техника подменила профессиональное мышление следователя или эксперта, а в том, чтобы стать его мощным усилителем, позволяющим сосредоточиться на смысловых, логических и тактических задачах расследования, делегируя рутину и обработку массивов данных надежным и понятным алгоритмам. Будущее технико-криминалистического обеспечения видится в формировании симбиоза человека и машины, где технологическая мощь служит строгому соблюдению закона и защите прав личности, что в конечном итоге и составляет высшую цель уголовного судопроизводства.

ЗАКЛЮЧЕНИЕ

Настоящее исследование, посвященное комплексному анализу роли информационно-коммуникационных технологий в технико-криминалистическом обеспечении, позволило сформулировать ряд выводов и обобщений, имеющих теоретическое и прикладное значение. В ходе работы последовательно решены поставленные задачи, что дает возможность представить целостную картину современного состояния, проблем и векторов развития указанной области.

Проведенный анализ позволяет утверждать, что технико-криминалистическое обеспечение в современных условиях представляет собой динамично развивающуюся, сложноорганизованную систему. Ее сущность раскрывается через единство трех взаимосвязанных компонентов: научно обоснованной совокупности технических средств, системы специальных знаний и методических рекомендаций по их применению, а также деятельности субъектов расследования и экспертных подразделений по использованию данного арсенала для достижения целей уголовного судопроизводства. Задачи технико-криминалистического обеспечения традиционно включали обнаружение, фиксацию, изъятие и исследование материальных следов преступления. Однако цифровая трансформация общества и преступной деятельности вносит в перечень этих задач принципиальные коррективы. Сегодня на первый план выходит работа с электронными следами, которые зачастую становятся центральным звеном в цепи доказательств.

Система технико-криминалистического обеспечения перестала быть лишь вспомогательным приложением к следственной практике; она трансформировалась в необходимую среду, в которой происходит большая часть процессуальных действий, от обнаружения информации до ее представления в суде. Указанная система носит открытый характер, постоянно пополняясь новыми инструментами, что требует от ее теоретического осмысления и правового регулирования высокой степени адаптивности.

Рассмотрение места и роли информационно-коммуникационных технологий в рамках данной системы демонстрирует их переход от периферийного инструментария к статусу системообразующего фактора. Информационно-коммуникационные технологии более не являются просто одним из классов технико-криминалистических средств; они выступают в качестве универсальной платформы, инфраструктурной основы, на которой строится и функционирует весь комплекс технико-криминалистического обеспечения. Роль этих технологий проявляется на нескольких уровнях. На оперативно-тактическом уровне они предоставляют конкретные инструменты для решения задач каждого этапа расследования. На стратегическом уровне информационно-коммуникационные технологии меняют саму парадигму расследования, смещая акцент с реактивного реагирования на проактивный анализ данных и прогнозное моделирование. На организационно-управленческом уровне они формируют новую логику взаимодействия между участниками процесса, обеспечивая дистанционную коммуникацию, электронный документооборот и централизованный доступ к информационным ресурсам. Следовательно, место информационно-коммуникационных технологий в системе технико-криминалистического обеспечения является центральным и интегративным, поскольку они пронизывают и связывают между собой все ее традиционные элементы, придавая им новое качество и возможности.

Выполненная классификация и характеристика информационно-коммуникационных технологий, используемых на основных этапах расследования, подтверждает их полифункциональность и адаптивность к потребностям следственной практики. В основе предложенной систематизации лежит функционально-процессуальный принцип, позволяющий соотнести конкретные технологии с типичными задачами, решаемыми в ходе досудебного производства.

На стадии возбуждения уголовного дела доминируют технологии информационно-справочного характера, обеспечивающие быстрый доступ к

учетным системам, и средства первичного анализа цифровых носителей, поступающих с заявлением о преступлении. Значение имеет и применение систем межведомственного электронного взаимодействия, позволяющих в сжатые сроки, установленные законом, собрать необходимые для принятия решения документы.

На этапе предварительного расследования арсенал используемых технологий становится максимально широким и дифференцированным. Он включает в себя специализированные средства фиксации обстановки места происшествия, среди которых особую ценность представляют технологии 3D-сканирования и панорамной съемки, создающие объективную и интерактивную цифровую модель.

Критическую важность приобретают аппаратно-программные комплексы для изъятия и исследования данных с электронных устройств, составляющие ядро современной цифровой криминалистики. Аналитические платформы для работы с большими данными и системы искусственного интеллекта для распознавания образов становятся незаменимыми помощниками при выдвижении и проверке версий.

Коммуникационные технологии, в особенности системы видео-конференц-связи, легализованные последними поправками в УПК РФ, кардинально меняют процедуру проведения следственных действий, делая ее более гибкой и экономичной.

На судебных стадиях фокус смещается в сторону технологий визуализации и презентации доказательств, превращающих сложные массивы информации в наглядные и убедительные материалы для суда. Представленная классификация, несмотря на условность границ между отдельными группами, подтверждает тезис о том, что современное расследование представляет собой высокотехнологичный процесс, эффективность которого напрямую зависит от грамотного и комплексного применения всего спектра информационно-коммуникационных средств.

Анализ актуальных проблем развития использования информационно-

коммуникационных технологий в технико-криминалистическом обеспечении выявил наличие серьезных системных вызовов, носящих правовой, организационный, кадровый и этический характер.

1. Наиболее острой остается проблема правовой регламентации. Несмотря на прогрессивные изменения в законодательстве, легализующие электронный документооборот и дистанционные форматы, процедурные основы применения многих передовых технологий, таких как алгоритмы прогнозной аналитики или средства криптографического анализа, остаются недостаточно урегулированными. Данное обстоятельство создает риски оспаривания доказательств, полученных с их помощью, и порождает правовую неопределенность для правоприменителей.

2. Существенным препятствием выступает хроническое технологическое отставание правоохранительных органов от быстро адаптирующихся криминальных структур, особенно в сфере финансовых технологий и средств анонимизации. Методическая разобщенность, выражающаяся в отсутствии единых стандартов работы с цифровыми следами на всех этапах их жизненного цикла, ведет к ошибкам и снижению доказательственной ценности изымаемой информации.

3. Кадровый дефицит, проявляющийся в нехватке специалистов, обладающих глубокими познаниями как в юриспруденции, так и в компьютерных науках, сводит на нет потенциал даже самого современного оборудования.

4. Наконец, этические дилеммы, связанные с риском установления режима тотального наблюдения при повсеместном использовании систем распознавания лиц и анализа больших данных, требуют проведения взвешенной общественной дискуссии и выработки надежных правовых гарантий защиты приватности граждан.

Указанные проблемы носят взаимосвязанный характер, и их игнорирование может привести к дисфункции всей системы технико-криминалистического обеспечения в условиях цифровой реальности.

Перспективы развития рассматриваемой области, однако, представляются значительными и связаны с комплексным преодолением выявленных трудностей.

1. Основной вектор видится в конвергенции технологий и создании единой цифровой экосистемы поддержки расследования. Ее ядром могла бы стать национальная платформа, интегрирующая разрозненные информационные ресурсы, аналитические инструменты и средства автоматизации рутинных процессуальных действий. Развитие технологий интернета вещей, распределенных реестров и квантовых вычислений откроет новые возможности для работы с ранее недоступными видами цифровых следов и создания неуязвимых систем защиты цепочки доказательств.

2. Критически важным направлением станет опережающая подготовка и переподготовка кадров, предполагающая тесную интеграцию юридического образования с программами в области информационной безопасности и анализа данных.

3. Законодательная база должна приобрести более гибкий, рамочный характер, устанавливая не запреты на использование новых технологий, а принципы и процедуры, гарантирующие их законность, обоснованность и проверяемость.

Таким образом, проведенное исследование подтверждает центральную роль информационно-коммуникационных технологий в модернизации технико-криминалистического обеспечения. От эффективности и скоординированности действий законодателя, научного сообщества и правоохранительных органов по преодолению существующих проблем и реализации намеченных перспектив будет зависеть способность системы уголовной юстиции выполнять свои функции в условиях беспрецедентных технологических и социальных изменений. Будущее технико-криминалистического обеспечения заключается в его способности эволюционировать, оставаясь при этом надежным гарантом установления истины и защиты прав личности в цифровом мире.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

I. Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 01.07.2020 № 11-ФКЗ, от 06.10.2022) // Собр. законодательства Рос. Федерации. – 2022. – №11. – Ст.1416.

2. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ: федеральный закон от 30.12.2001 № 195-ФЗ // Собрание законодательства Российской Федерации. – 2002. – № 1 (ч. 1). – Ст. 1.

3. Уголовно-процессуальный кодекс Российской Федерации: федеральный закон от 18.12.2001 № 174-ФЗ // Собрание законодательства Российской Федерации. – 2001. – № 52 (ч. 1). – Ст. 4921.

4. Уголовный кодекс Российской Федерации: федеральный закон от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации. – 1996. – № 25. – Ст. 2954.

5. О полиции: федеральный закон от 07.02.2011 № 3-ФЗ: // Собрание законодательства Российской Федерации. – 2011. – № 7. – Ст. 900.

6. О несении службы участковым уполномоченным полиции на обслуживаемом административном участке и организация этой деятельности: приказ МВД России от 29 марта 2019 г. № 205 [Электронный ресурс]. URL: www.pravo.gov.ru (дата обращения: 12.01.2026).

II. Учебная, научная литература

1. Амиров, Р.Г., Еремченко, В.И. Проблемы использования современных информационных технологий в расследовании преступлений // Евразийский юридический журнал. – 2023. – № 11. – С. 365-366.

2. Ардавов, М.М. О проблемных аспектах применения

информационных технологий в расследовании преступлений // Право и управление. – 2025. – № 7. – С. 132-135.

3. Архипова, П.С. Отдельные проблемы использования информационных технологий в расследовании преступлений // Студенческий вестник. – 2024. – № 11. – С. 20-22.

4. Асылбек, Д.Е., Тилеубергенов Е.М. Использование новых информационных технологий при раскрытии и расследовании преступлений // Трансформация российской науки в эпоху информационного общества: сборник научных трудов. – М., 2025. – С. 155-158.

5. Ашихмина, В.С. Использование специальных знаний при расследовании преступлений, совершаемых с использование информационных технологий: актуальные проблемы и перспективы развития // Технико-криминалистическое обеспечение раскрытия и расследования преступлений: сборник научных статей. – М., 2024. – С. 352-355.

6. Береза, К.Ю. Использование искусственного интеллекта и информационных технологий в ходе расследования уголовных дел // Государство, право, экономика: история и современность: сборник научных трудов. – Краснодар, 2025. – С. 69-73.

7. Брезгулевская, А.А., Шлапакова, В.А. Информационные системы и технологии в криминалистике: как компьютерный прогресс повлиял на уголовные расследования // Современные вопросы устойчивого развития общества в эпоху трансформационных процессов: сборник научных трудов. –М., 2023. – С. 146-151.

8. Быстрова, Ю.В., Ганаева, Е.Э. IT-технолгии в раскрытии и расследовании преступлений // Вестник Чеченского государственного университета им. А.А. Кадырова. – 2023. – № 2. – С. 96-101.

9. Вихрова, Л.Ю., Кушнир И.А. Эффективность применения информационных технологий в предварительном расследовании преступлений // Актуальные проблемы предварительного расследования: сборник научных трудов. – СПБ., 2023. –С. 127-129.

10. Воробьев, Д.С. Современное использование информационных технологий в раскрытии и расследовании преступлений // Неделя российской науки в Рязанском филиале Московского университета МВД России имени В.Я. Кикотя: сборник научных трудов. – Рязань, 2025. – С. 402-406.

11. Губарева, А.С. Перспективы и риски использования информационных технологий при расследовании преступлений // Научный альманах. – 2025. – № 6. – С. 72-74.

12. Долженко, Н.И., Подмоков, Н.С. Информационные технологии как криминалистические средства расследования и борьбы с преступностью // Тенденции развития науки и образования. – 2024. – № 6. – С. 119-121.

13. Жбанов, Д.О. Применение цифровых технологий в криминалистике // Студенческий вестник. – 2023. – № 46. – С. 39-41.

14. Казакова, В.С. Роль информационных технологий при расследовании преступлений // Научный поиск курсантов: сборник научных трудов. – Могилев, 2025. – С. 96-97.

15. Казанцев, С.Я., Романова, Г.В. К вопросу об использовании информационно-поисковых технологий в работе следователя // Криминологический журнал. – 2025. – № 3. – С. 73-78.

16. Калюжный, А.Н. Векторы реализации потенциала информационных технологий в деятельности оперативных и следственных подразделений // Вестник Восточно-Сибирского института МВД России. – 2025. – № 2. – С. 140-149.

17. Кислицына, А.Е., Зятюк, Б.И. Методология использования информационных технологий в расследовании // Моя профессиональная карьера. – 2025. – № 71. – С. 165-171.

18. Кравченко, Е.В., Пухкалова, М.О. Проблемные аспекты применения информационных технологий в расследовании преступлений в цифровом пространстве // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. – 2024. – № 2. – С. 114-117.

19. Кудинова, А.А. Использование цифровых технологий в раскрытии и

расследовании преступлений: современное состояние и перспективы совершенствования // Юстиция. – 2023. – № 1. – С. 112-119.

20. Кудинова, А.А., Тюергалиева, А.Е. Возможности и перспективы использования цифровых технологий в деятельности следственных органов // Современные научные исследования: сборник научных статей. – Пенза, 2023. – С. 69-73.

21. Распопова, П.В. Роль информационного обеспечения и информационных технологий в раскрытии и расследовании преступлений // Актуальные проблемы науки и практики. – 2025. – № 52. – С. 133-135.

22. Рахмонбердиев, Б.Б. Применение информационных технологий в органах предварительного расследования // Уголовное судопроизводство России и зарубежных государств: проблемы и перспективы развития: сборник научных трудов. – СПб., 2023. –С. 659-662.

23. Романюк, Е.В., Шостак Д.Т. Перспективы использования информационных технологий при расследовании преступлений // Молодой ученый. – 2022. – № 3. – С. 113-120.

24. Садовская, В.В. Использование информационных технологий при расследовании современных преступлений // Уголовно-правовое обеспечение правоохранительной деятельности: сборник научных статей. –М., 2024. – С. 90-94.

25. Селютин, Д.М. Методология использования информационных технологий в расследовании преступлений // Молодой ученый. – 2025. – № 3. – С. 17-19.

26. Семенова, И.В. Цифровая криминалистика: криминалистические инструменты и технологии, применяемые при проведении расследований // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. – 2025. – № 2. – С. 377-383.

27. Соломатина, А.Г. Использование информационных технологий при расследовании преступлений // Уголовное судопроизводство России и зарубежных государств: проблемы и перспективы развития: сборник

научных трудов. – СПб., 2023. –С. 304-309.

28. Суетина, П.А. Использование информационно-коммуникационных технологий в расследовании преступлений // Современные достижения молодых исследователей: сборник научных трудов. – Пенза, 2023. – С. 88-92.

29. Таашев, Д.Б. Проблемные аспекты применения информационных технологий в расследовании преступлений в цифровом пространстве // Российский научный вестник. – 2025. – № 4. – С. 252-254.

30. Тайтубаева, Л.М. Понятие информационных технологий и их значение при использовании в ходе расследования преступлений // Право и управление. – 2025. – № 6. – С. 236-242.

31. Фролов, В.В. Использование информационных технологий в расследовании: направления, проблемы и перспективы // Полицейская и следственная деятельность. – 2023. – № 2. – С. 3-13.

32. Харитонов, С.А. Использование инновационных технологий в расследовании преступлений по «горячим следам» // Новые вызовы – новые исследования: сборник научных статей. – Петрозаводск, 2022. – С. 94-101.

33. Шигапова, Л.Р. Применение современных информационных технологий на этапе предварительного расследования // Моя профессиональная карьера. – 2023. – № 55. –С. 207-210.

34. Шкарина, Е.И., Криницин, Н.Н. Возможности использования искусственного интеллекта при расследовании преступлений // Мировые научные дискуссии в эпоху цифровизации: сборник научных статей. – Рязань, 2023. – С. 419-420.

35. Яковлева, А.С. Использование современных информационных технологий в судебно-экспертной деятельности и дактилоскопии в частности // Судебная экспертиза и исследования. – 2022. – № 2. – С. 105-107.

III. Эмпирические материалы

1. О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и

гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации): Постановление Пленума Верховного Суда РФ от 25.12.2018 № 46 [Электронный ресурс]. URL: www.pravo.gov.ru (дата обращения: 12.01.2026).

2. О практике применения законодательства при рассмотрении уголовных дел в суде первой инстанции (общий порядок судопроизводства): Постановление Пленума Верховного Суда РФ от 19.12.2017 № 51 [Электронный ресурс]. URL: www.pravo.gov.ru (дата обращения: 12.01.2026).

ПРИЛОЖЕНИЕ

АНКЕТА

Уважаемый коллега!

Просим Вас принять участие в анонимном опросе, посвященном оценке роли и эффективности использования информационно-коммуникационных технологий (ИКТ) в технико-криминалистическом обеспечении расследования преступлений. Ваше мнение важно для формирования объективной картины и определения перспектив развития данного направления.

1. Какова, по Вашему мнению, общая значимость информационно-коммуникационных технологий для успешного расследования преступлений сегодня?

- Крайне высокая, без них расследование невозможно.

- Высокая, они существенно помогают.

- Умеренная, являются полезным дополнением.

- Незначительная, традиционные методы эффективнее.

2. Какие из перечисленных ИКТ Вы используете в своей практике регулярно (несколько раз в месяц)? (Возможно несколько вариантов ответа)

- Специализированные программные комплексы (например, для составления схем, фотосъемки, работы с базами данных).

- Системы видеоконференцсвязи для взаимодействия с другими органами и судами.

- Средства криптографической защиты служебной информации.

- Мобильные устройства и приложения для выезда на место происшествия.

- Аппаратно-программные комплексы для изъятия и предварительного анализа данных с электронных носителей.

- Другое (укажите, пожалуйста): _____

3. С какой целью Вы используете ИКТ наиболее часто? (Выберите не более двух основных)

- Фиксация обстановки места происшествия (3D-сканирование,

панорамная съемка).

- Поиск и проверка информации в оперативно-справочных и розыскных учетах.

- Анализ больших массивов данных (например, финансовых транзакций, соединений абонентов).

- Коммуникация и оперативный обмен информацией с другими участниками процесса.

- Документирование хода и результатов следственных действий.

- Экспертная деятельность и взаимодействие с экспертно-криминалистическими подразделениями.

4. Как Вы оцениваете уровень технической оснащенности Вашего подразделения необходимыми ИКТ?

- Полностью соответствует современным задачам.

- В основном соответствует, но есть отдельные недостатки.

- Частично соответствует, требуется существенное обновление.

- Практически не соответствует современным требованиям.

5. Достаточен ли уровень Вашей подготовки для эффективного использования имеющихся ИКТ?

- Да, моих знаний и навыков вполне хватает.

- В основном да, но по некоторым новым технологиям нужны дополнительные курсы.

- Затрудняюсь ответить.

- Нет, чувствую значительный дефицит знаний, навыки носят фрагментарный характер.

6. Как часто возникают технические проблемы (сбои ПО, несовместимость, низкая скорость), затрудняющие использование ИКТ в работе?

- Ежедневно или несколько раз в неделю.

- Несколько раз в месяц.

- Достаточно редко, раз в несколько месяцев.

- Практически никогда.

7. Насколько, по Вашему опыту, использование ИКТ сокращает временные затраты на выполнение отдельных процессуальных действий?

- Существенно сокращает (более чем на 30%).

- Умеренно сокращает (примерно на 10-30%).

- Не оказывает значительного влияния на сроки.

- Иногда даже увеличивает временные затраты из-за сложности.

8. Способствует ли, на Ваш взгляд, использование ИКТ (электронные носители, видеозаписи) повышению объективности и непредвзятости доказательственной базы?

- Да, в значительной степени, так как информация фиксируется полно и неизбирательно.

- Скорее да, но требуется строгий процессуальный контроль.

- Затрудняюсь ответить.

- Нет, традиционные протоколы и вещественные доказательства надежнее.

9. Сталкивались ли Вы с проблемой противодействия использованию ИКТ со стороны лиц, причастных к преступной деятельности (например, использование шифрования, уничтожение цифровых следов)?

- Да, постоянно, это серьезная проблема.

- Да, периодически.

- Редко.

- Не сталкивался.

10. Какие направления развития ИКТ, на Ваш прогноз, будут наиболее востребованы в следственной практике в ближайшие 3-5 лет? (Возможно несколько вариантов)

- Искусственный интеллект для анализа данных и выявления связей.

- Прогнозная аналитика и моделирование криминальных ситуаций.

- Расширенное использование биометрических технологий.

- Автоматизация рутинных процессов документооборота.

- Развитие облачных платформ для межведомственного взаимодействия.

- Средства анализа информации из открытых источников (OSINT).

11. Что, по Вашему мнению, является главным препятствием для более широкого и эффективного внедрения ИКТ в следственную практику? (Выберите не более двух)

- Недостаточное финансирование и устаревшая материально-техническая база.

- Дефицит специальных знаний и навыков у сотрудников.

- Консерватизм и неготовность к изменениям в организации работы.

- Проблемы информационной безопасности и защиты данных.

- Излишне бюрократизированные процедуры внедрения новых решений.

- Несовершенство законодательной базы, регулирующей использование цифровых доказательств.

12. Ваш стаж работы в следственных подразделениях:

- До 3 лет.

- От 3 до 10 лет.

- Более 10 лет.

Благодарим за участие!

Материал вычитан, цифры, факты, цитаты сверены с первоисточником. Материал не содержит сведений, составляющих государственную и служебную тайну И.В. Ширина