Полицейская деятельность
Правильная ссылка на статью:
Вяткин А.А. Ключевые аспекты прокурорского надзора за исполнением законов органами дознания и предварительного следствия при расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий // Полицейская деятельность. 2025. № 5. С. 11-24. DOI: 10.7256/2454-0692.2025.5.76305 EDN: NNITRI URL: https://nbpublish.com/library_read_article.php?id=76305

Ключевые аспекты прокурорского надзора за исполнением законов органами дознания и предварительного следствия при расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий

Вяткин Андрей Анатольевич

ORCID: 0000-0002-3169-5111

старший преподаватель; кафедра Прокурорского надзора и участия прокурора в рассмотрении гражданских и арбитражных дел; Иркутский юридический институт (филиал) Университета прокуратуры Российской Федерации

664035, Россия, Иркутская область, г. Иркутск, ул. Шевцова, 1

viatkin-chita@yandex.ru

Статья из рубрики "Контроль деятельности полиции"

DOI:

10.7256/2454-0692.2025.5.76305

EDN:

NNITRI

Дата направления статьи в редакцию:

16-10-2025

Дата публикации:

23-10-2025

Аннотация: Предметом исследования выступают ключевые аспекты прокурорского надзора за исполнением законов органами дознания и предварительного следствия при расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Объектом исследования является деятельность органов прокуратуры в рамках надзора за исполнением законов органами предварительного расследования в условиях цифровизации и появления

высокотехнологичных преступлений. Автор рассматривает современное состояние преступности, характеризующееся увеличением числа преступлений, совершенных с использованием цифровых технологий, и низкой раскрываемостью таких преступных деяний. Подробно анализируется специфика прокурорского надзора в условиях цифровизации. Особое внимание уделяется значимости взаимодействия органов предварительного расследования с оперативными подразделениями и эффективного применения результатов их деятельности. Автор также акцентирует внимание на международном сотрудничестве в борьбе с трансграничными преступлениями. Методология данного научного исследования основывается на комплексном подходе, сочетающем теоретический анализ и практическое осмысление проблематики прокурорского надзора в условиях цифровизации. Применяется метод системного анализа, направленного на изучение взаимосвязей между различными компонентами прокурорской деятельности в обозначенной сфере и деятельностью органов предварительного расследования. Эмпирические данные подкрепляются ссылками на научные труды. Основные выводы проведенного исследования заключаются в том, что современная цифровизация общества значительно усложнила задачи прокурорского надзора, особенно в контексте надзора за расследованием преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Автор подчеркивает, что традиционные подходы к прокурорскому надзору требуют существенной адаптации, поскольку современные преступления характеризуются высоким уровнем технологичности, анонимности и трансграничности, что ставит перед органами прокуратуры новые вызовы. Исследование выявило необходимость повышения уровня компетенций прокуроров, включая знания в области криминалистики, оперативно-розыскной деятельности в цифровой среде и информатики. Новизна исследования заключается в полученных результатах системного анализа ключевых аспектов прокурорского надзора в условиях цифровизации. Автор пришел к выводу о том, что эффективность современного прокурорского надзора за исполнением законов органами дознания и предварительного следствия при расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий, может быть повышена за счет его комплексного характера, акцентирования внимания в его организации и осуществлении на выявленных ключевых аспектах.

Ключевые слова:

прокурорский надзор, информационно-телекоммуникационные технологии, расследование киберпреступлений, технологичная преступность, следствие и дознание, современная преступность, процессуальный надзор, оценка полноты расследования, проблемы прокурорского надзора, компьютерные преступления

Развитие информационно-телекоммуникационных технологий существенно повлияло практически на все сферы общественных отношений, за минувшее десятилетие существенно изменилась и преступность. Высокотехнологичными становятся способы совершения даже привычных и традиционных преступлений.

В таких условиях работа правоохранительных органов и прокуратуры существенно усложнилась, об этом свидетельствуют отдельные статистические показатели. Так, согласно сведениям Министерства внутренних дел Российской Федерации о преступности за январь-июль 2025 года число зарегистрированных в Российской Федерации преступлений, совершённых с использованием информационно-телекоммуникационных

технологий или в сфере компьютерной информации, остаётся значительным – 424851. Вместе с тем, их раскрываемость составляет лишь 28,9 %. Следует отметить, что данный показатель является для прокуроров определённым сигналом к повышению эффективности мер координационного характера и проверки материалов уголовных дел соответствующей категории.

Результаты Всероссийской научно-практической конференции «Деятельность прокуратуры Российской Федерации в обеспечении законности в условиях современных вызовов», проведенной 20 февраля 2025 года Иркутским юридическим институтом (филиалом) Университета прокуратуры Российской Федерации, а также практика проведения занятий для слушателей факультета профессиональной переподготовки и повышения квалификации показывают, что существующий подход к организации и осуществлению прокурорского надзора за исполнением законов органами дознания и предварительного следствия при расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий, требует определённого переосмысления.

Современные преступники используют средства мобильной связи, компьютерную технику, сеть Интернет. Способы совершения преступлений, с учетом широкого спектра возможностей такой техники, довольно разнообразны и постоянно изменяются. Более того, виртуальное пространство позволяет действовать анонимно, совершать трансграничные преступления. Именно с этим связаны основные сложности как раскрытия, расследования указанных преступлений, так и соответствующего прокурорского надзора.

В связи с этим, с учётом доступных для научной статьи объемов исследования, считаем необходимым выявить ключевые аспекты такого надзора, от которых зависит его эффективность.

1. Криминалистические аспекты прокурорского надзора.

В пункте 4.4 «Концепции воспитательной работы в системе прокуратуры Российской Федерации», утверждённой приказом Генерального прокурора Российской Федерации от 17.03.2010 № 114 указано, что появление новых видов преступлений и иных правонарушений требует от прокурорских работников наличия специальных знаний в области рыночной экономики, информационного, налогового, банковского, страхового, экологического и другого отраслевого законодательства, а также владения современными методиками расследования и проведения прокурорских проверок. Их недостаточность вызывает неуверенность работников прокуратуры, влияет на качество и эффективность работы.

Мы полностью согласны с позицией Генеральной прокуратуры Российской Федерации и считаем, что исполнение требований данной нормы играет важное значение в организации и осуществлении прокурорского надзора обозначенной специфики. Вместе с тем, оценивая его современные реалии, возможно констатировать, что при изучении материалов уголовных дел прокуроры практически не опираются на методики расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Обычно они ориентируются на положения уголовного, уголовно-процессуального законодательства и комментарии к нему, а также на положительные примеры следственной и судебной практики. В связи с этим, их работа по оценке полноты материалов уголовных дел, содержания следственных действий нуждается в систематизации.

О роли методик расследования достаточно ёмко и точно сказано учёными Университета прокуратуры Российской Федерации: «знание прокурором вопросов методики и тактики расследования преступлений, выполнения отдельных следственных действий, использования технико-криминалистических средств, возможностей судебных экспертиз и специальных знаний позволяет эффективно выполнять возложенные на него законом обязанности по обеспечению полноты, всесторонности и объективности предварительного расследования» [1, с.238].

Мы не только поддерживаем данную точку зрения, но и считаем, что без использования в прокурорском надзоре результатов научных работ в области современной криминалистики повысить его эффективность не представляется возможным. Для изучения материалов уголовного дела о преступлении, совершенном с использованием информационно-телекоммуникационных технологий, прокурору как минимум необходимо знать его криминалистическую характеристику. А. Ю. Головин, О. П. Грибунов, А. А. Бибиков отмечают, что она представляет собой сложную систему типовых сведений, которые позволяют раскрыть закономерности и процессы совершения общественно-опасных явлений, особенности поведения участников противоправного события, влияние на совершение преступления пространственно-временных и окружающих условий, а также противодействие раскрытию и расследованию преступлений [2, с.17]. Прокурору важно понимать специфику виртуальной обстановки, типичных способов совершения преступлений, особенности личности преступника.

Отдельного внимания заслуживают цифровые следы. В. Б. Вехов под «электронно-цифровым следом» понимает любую криминалистически значимую компьютерную информацию, т.е. сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе с помощью электромагнитных взаимодействий либо передающиеся по каналам связи посредством электромагнитных сигналов [3, с.658].

Дополним данное определение выводом, к которому пришел А. Г. Волеводз: «при расследовании преступлений, совершаемых с применением компьютерных сетей, могут использоваться их следы, представляющие собой сведения о прохождении информации по проводной, радио-, оптической и другим электромагнитным системам связи (электросвязи), которые носят обобщенное название «сведения о сообщениях, передаваемых по сетям электрической связи (электросвязи)», либо сохраняемые поставщиками услуг (провайдерами) «исторические данные» о состоявшихся сеансах связи или переданных сообщениях, либо «данные о потоках» или «данные о потоках информации». Во многих случаях компьютерная информация может находиться в стадии как хранения, так и передачи, либо переходить из одной стадии в другую. [4, с.10].

Изложенное указывает на два важнейших свойства цифровой информации. Во-первых, она имеет связь с материальным носителем. Во-вторых, она может существовать как в статическом состоянии (храниться на материальном носителе), так и в динамическом - передаваться по каналам связи. В совокупности изложенное указывает на возможность работы с двумя разными состояниями такой информации в рамках следственных действий. Например, информация в статическом состоянии может быть подвергнута осмотру, а перехват данных, передающихся по каналу связи, может быть обеспечен оперативно-розыскными органами в рамках исполнения поручения следователя.

Соответственно, понимание прокурором специфики цифровых следов может существенно влиять на его подход к оценке полноты и своевременности проведения следственных

действий по уголовному делу.

Значительный объем отличительных особенностей преступлений, совершенных с использованием информационно-телекоммуникационных технологий, их новизна повлекли создание цифровой криминалистики как частной криминалистической теории. Так, В. Б. Вехов и С. В. Зуев отмечают, что её объектом являются правонарушения, связанные с использованием компьютерных технологий; общественные отношения, возникающие в ходе выявления, раскрытия, расследования и предупреждения правонарушений, когда осуществляется обнаружение, фиксация, предварительное исследование, использование компьютерной информации и средств ее обработки; деятельность по разработке криминалистических приемов, методов, средств использования компьютерных технологий в борьбе с правонарушениями [5, с.15].

Также важную роль в раскрытии, расследовании преступлений, совершённых с использованием информационно-телекоммуникационных технологий, играет компьютерная экспертиза, возможности и потенциал которой трудно переоценить. По нашему мнению, наиболее универсальная классификация предложена Е. Р. Россинской, которая разделяет компьютерно-техническую экспертизу на аппаратно-компьютерную, программно-компьютерную, информационно-компьютерную (исследование данных) и компьютерно-сетевую экспертизы, в основе чего лежит аппаратное, техническое, программное или информационное обеспечение компьютерного средства [6, с.140]. Надзирающему прокурору, в свою очередь, необходимо понимать специфику назначения такой экспертизы, содержание вопросов, которые могут быть поставлены при её назначении. От этого зависят не только её результаты, но и сроки проведения.

В каждом случае законность принятых процессуальных решений оценивается прокурором с точки зрения полноты расследования и принятых следственными органами мер по установлению подлежащих доказыванию обстоятельств. Соответственно критерии такой оценки, по нашему мнению, не могут быть сформированы без учета методики раскрытия, расследования преступлений соответствующей категории.

Стремительный процесс цифровизации, появление новых видов экономической деятельности создают необходимость использования прокурором не только таких методик, но и специальных знаний. Уже сегодня прокурору нужно иметь хотя бы минимальные знания в области информационной безопасности и функционирования современной электронно-вычислительной техники. В ближайшем будущем без соответствующих цифровых компетенций самостоятельное изучение прокурором материалов таких уголовных дел станет попросту невозможным.

2. Оперативно-розыскная деятельность в киберпространстве.

В современных условиях борьбы с технологичной преступностью заметно возросла роль доказательств, которые формируются на основе результатов оперативно-розыскной деятельности. Как отмечает В. С. Овчинский, преступность, терроризм, коррупция, отмывание денег становятся цифровыми. Одновременно сама оперативно-розыскная деятельность уже в большой мере стала цифровым инструментом борьбы с перечисленными явлениями [7, с.13].

Соответственно, рассекреченные и представленные следователю материалы не могут остаться без внимания со стороны надзирающего прокурора. Исходя из этого для прокурорского надзора важны вопросы взаимодействия органов предварительного расследования с оперативными подразделениями, подготовки качественных

следственных поручений о проведении оперативно-розыскных мероприятий. Каждое составленное следователем поручение должно учитывать не только вероятные результаты его выполнения, но и возможности оперативных подразделений, которые могут позволить решить конкретную задачу.

Так, отдельная работа может быть проведена оперативными подразделениями в отношении цифровых данных, находящихся в открытых источниках сети Интернет. В современной науке методы и инструменты, которые позволяют работать с такими данными, объединены технологией Open Source Intelligence (OSINT), что возможно перевести как «разведка по открытым источникам».

Достаточно точное описание её роли в процессе раскрытия, расследования преступлений приведено А. А. Бессоновым. Данный учёный поясняет, что суть этой технологии состоит в мониторинге с использованием информационно-аналитических методов (Data Mining) открытых источников информационно-телекоммуникационной среды и элементов ее инфраструктуры в целях поиска, обнаружения и фиксации криминалистически значимой информации, связанной с подготавливаемым, совершаемым или совершенным преступлением (преступлениями) [8, с.261].

Н. А. Архипова, О. В. Кругликова, А. В. Шебалин, М. О. Янгаева в учебном пособии, посвящённом расследованию хищений, совершенных с использованием информационно-телекоммуникационных технологий, отмечают, что с помощью OSINT можно не только проводить сбор данных в социальных сетях, но также использовать расширенные запросы поисковых систем для предоставления наиболее точных результатов поиска, осуществлять поиск удаленных версий веб-сайтов, отслеживать людей и их деятельность в интернете с помощью общедоступных баз данных и эффективных инструментов поиска, просматривать спутниковые изображения любой улицы мира, искать геолокацию лица и многое другое [9, с.21].

Отметим, что на основе полученных с использованием OSINT результатов могут быть организованы оперативно-технические мероприятия, позволяющие получить удалённый доступ к закрытой информации на электронных устройствах преступника или на удалённых серверах (например, с использованием возможностей Бюро специальный технических мероприятий), возможно проведение полноценных тактических операций, направленных на установление его личности.

Более того, пунктами 1.2 и 1.3 приказа Генерального прокурора Российской Федерации от 16.01.2012 № 7 «Об организации работы органов прокуратуры Российской Федерации по противодействию преступности» прокурорам предписано особое внимание обращать на исполнение поручений органов предварительного расследования и использование результатов оперативно-розыскной деятельности, тщательно проверять полноту принимаемых оперативными подразделениями мер при решении задач по выявлению, предупреждению, пресечению и раскрытию преступлений, установлению лиц, их подготавливающих, совершающих или совершивших. Сложно представить неукоснительное выполнение прокурором данных требований в условиях отсутствия знаний в области современной теории оперативно-розыскной деятельности и без понимания специфики проведения оперативно-розыскных мероприятий в виртуальном пространстве сети Интернет.

3. Международное сотрудничество в сфере уголовного судопроизводства.

Многие технологичные преступления носят трансграничный характер. Е. В. Рогова

совершенно верно отмечает, что в противодействии киберпреступности большое значение имеет международное сотрудничество. При этом следует расширять обмен опытом, изучать эффективную практику иных государств в целях выработки совместных методов, способствующих кибербезопасности [10, с.89]. Мы поддерживаем данную точку зрения и считаем необходимым дополнить, что для раскрытия и расследования таких преступлений особенно важен такой уголовно-процессуальный механизм как оказание правовой помощи.

Пунктом 1.12 упомянутого ранее приказа прокурорам предписано принимать исчерпывающие меры по выполнению обязательств и реализации прав, вытекающих из международных договоров Российской Федерации в сфере уголовного судопроизводства и борьбы с преступностью в части компетенции органов прокуратуры. В связи с этим, отдельным аспектом проверки материалов уголовных дел о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий, является изучение прокурором имеющихся в деле запросов о правовой помощи и результатов их выполнения. Отдельное внимание должно быть уделено особенностям международного взаимодействия в рамках функционирования Интерпола, по каналам которого могут направляться запросы в соответствии с пунктами 95 и 97 приказа МВД РФ № 786, Минюста РФ № 310, ФСБ РФ № 470, ФСО РФ № 454, ФСКН РФ № 333, ФТС РФ № 971 о 06.10.2006 «Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола».

Виртуальное пространство не имеет материальных, географических границ. Сетевые серверы, компьютеры преступника и жертвы могут находиться на территории разных государств. В таких условиях у органов предварительного расследования возникают различные трудности. Например, К. К. Клевцов в своей научной статье раскрыл содержание проблемы установления поставщика услуг, который может предоставить цифровые данные. Она существует в силу дифференциации географического расположения серверов и центров обработки данных, в частности облачных услуг. Зачастую физическое оборудование, которое предоставляет облачные услуги, находится в местах для обработки данных, стратегически расположенных для минимизации задержек в предоставлении таких услуг, а также затрат на электроэнергию и охлаждение оборудования [11, с.658]. Также к числу проблем возможно отнести: отличия законодательства различных государств, которые касаются ответственности за компьютерные преступления; длительное выполнение запросов; отсутствие в запросах и в ответах на них необходимой информации; отличия уголовно-процессуального законодательства государств, регламентирующего процедуры получения доказательств.

Соответственно, прокурор при изучении материалов уголовного дела может столкнуться с подобными вопросами и должен будет сделать обоснованный вывод о целесообразности принятия мер реагирования в конкретной ситуации. Также прокурору важно понимать особенности использования в процессе доказывания материалов, которые получены за рубежом.

Безусловно, правовая помощь является лишь частью механизма международного сотрудничества в сфере уголовного судопроизводства. В настоящий момент в сфере международной борьбы с киберпреступностью происходят существенные изменения, а именно 24 декабря 2024 года Генеральная Ассамблея ООН одобрила «Конвенцию против киберпреступности; Укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме,

относящимися к серьезным преступлениям». Этот международный договор повлияет на национальное законодательство государств-участников и в целом на международную практику раскрытия, расследования компьютерных преступлений. Фактически создаётся универсальный международный механизм борьбы с такими преступлениями, что должно позволить повысить их раскрываемость.

Одна из важнейших глав конвенции «Процессуальные меры и правоприменение» содержит нормы, в которых перечислены универсальные мероприятия по раскрытию и расследованию компьютерных преступлений: оперативное обеспечение сохранности хранимых электронных данных; оперативное обеспечение сохранности и частичное раскрытие данных о трафике; распоряжение о предоставлении информации организациями; обыск и изъятие хранимых электронных данных; сбор в режиме реального времени данных о трафике; перехват данных о содержании электронных сообщений; замораживание, арест и конфискация доходов от преступлений и другие.

Постепенная наработка международной правоприменительной практики, на наш взгляд, неизбежно приведет к необходимости внесения соответствующих дополнений в методику проверки прокурором материалов уголовных дел о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий.

4. Финансовый мониторинг и криптовалюты.

Неотъемлемой частью киберпреступлений являются финансовые операции, в преступной среде набирает популярность криптовалюта как инструмент анонимных расчетов и легализации преступных доходов.

Важно отметить, что раскрытие и расследование таких преступлений тесно связано с функционированием системы финансовой разведки и противодействия легализации (отмыванию) полученных преступным путём доходов. О. Н. Тисен в своей монографии подробно описывает возможности Федеральной службы по финансовому мониторингу (Росфинмониторинга), раскрывает содержание взаимодействия службы с правоохранительными органами и отдельное внимание уделяет аналитическому программному инструменту «Прозрачный блокчейн». В частности, она отмечает, что на основании полученных с его помощью сведений о криптобиржах и обменниках инициируются проверочные запросы в адрес зарубежных подразделений финансовой разведки на предмет установления владельцев криптокошельков [12, с.169]. Кроме того, международно-правовые аспекты противодействия преступлениям, совершаемым с использованием криптовалют, достаточно подробно раскрыты Волеводзом А. Г., Васюковым В. Ф., Клевцовым К. К., Сидоренко Э. Л., Титовым А. А., Цыплаковой А. Д [13. с.193].

Прокурору в рамках изучения материалов уголовных дел следует уделять особое внимание данному вопросу, поскольку правоохранительные органы не всегда понимают особенности взаимодействия с Росфинмониторингом, направления в его адрес запросов, использования полученной от него информации и международного обмена информацией по линии финансовой разведки.

Однако обозначенная проблема, к сожалению, является не единственной. Особое внимание сложностям правоприменительной практики уделяет Генеральная прокуратура Российской Федерации не только по линии методического обеспечения, но и путём проведения научных исследований. Так, проблемы раскрытия, расследования преступлений, совершённых с использованием криптовалюты, а также её изъятия и

оценки исследовались М. М. Долгиевой [14, с.38] и И. А. Безенковым [15, с.48]. Их научные статьи носят практикоориентированный характер, содержат конкретные способы решения выявленных проблем и могут использоваться в прокурорском надзоре.

5. Уголовно-процессуальный аспект прокурорского надзора.

На первый взгляд требования уголовно-процессуального законодательства Российской Федерации достаточно универсальны, в целом прокурорами применяется довольно стандартный алгоритм проверки их исполнения при изучении материалов уголовных дел. Практика показывает, что прокуроры обычно ориентируются на перечень подлежащих доказыванию обстоятельств, общие условия предварительного расследования, порядок проведения различных следственных и процессуальных действий, формальные требования к оформлению документов, на перечень прав, которыми наделены участники уголовного судопроизводства, и т. д.

Вместе с тем, специфика досудебного производства по уголовным делам обозначенной категории требует от прокурора повышенного внимания к их изучению. Так, Н. В. Османова выделила характерные черты такого досудебного производства: начало досудебного производства по сообщению о преступлении, совершенном с использованием современных информационных и телекоммуникационных технологий, выражающееся в типичных поводах возбуждения уголовного дела и особенностями проведения проверки; уголовно-процессуальная специфика определения места совершения преступления и подследственности уголовных дел; особый предмет доказывания по уголовным делам о преступлениях, совершенных с использованием информационных и телекоммуникационных технологий; специальная процедура изъятия электронных носителей информации и копирования с них информации; установление информации о соединениях между абонентами и (или) абонентскими устройствами, используемыми в целях совершения преступления; обязательное взаимодействие следователя с органами дознания, администрацией социальных сетей, мессенджеров и др. [8, с.148].

Е. Р. Россинская и Т. А. Сааков не только выявили особенности следственных действий, направленных на формирование полученных на основе цифровой информации доказательств, но и сформулировали рекомендации для дознавателей и следователей при работе с такими доказательствами [16, с.121] Важно, что учёными продемонстрирована связь криминалистического аспекта с уголовно-процессуальным аспектом в контексте выявления цифровых следов и их процессуального закрепления в рамках проведения следственного действия.

Отдельного внимания, на наш взгляд, заслуживают особенности проведения осмотра цифровой информации в сети Интернет в режиме удалённого доступа. В целях обеспечения допустимости полученных в рамках такого следственного действия доказательств требуется документирование всех действий, проведённых с использованием электронных устройств и программного обеспечения, чтобы гарантировать прозрачность процесса и возможность проверки данных на предмет их корректности и достоверности. Должно быть зафиксировано какие именно методы были использованы при поиске информации, какие инструменты применялись, а также подробно описаны полученные результаты, включая ссылки на ресурсы, данные о дате и времени фиксации. Нельзя не упомянуть о необходимости подтверждения подлинности обнаруженных данных и проверки их неизменности.

Для проведения сложных осмотров, которые предусматривают использование

специализированного программного обеспечения, целесообразно привлечение специалиста.

Важно учесть, что современная отечественная наука уголовного процесса часто опережает практику. Этим обусловлена необходимость постоянного изучения прокурорами актуальных научных работ. Например, А. С. Смирновым по результатам анализа отечественного и зарубежного опыта уже сформулированы выводы о возможных изменениях в законодательстве Российской Федерации и в правоприменительной практике, которые коснутся использования электронных доказательств, электронного доказывания и применения искусственного интеллекта [17, с.30].

6. Уголовно-правовой аспект прокурорского надзора.

Е. В. Рогова и А. П. Перетолчин отмечают, что появление новых способов, средств совершения корыстных преступлений вызывает не только широкую дискуссию в научной среде, но и определенные затруднения при их квалификации правоприменительными органами в рамках действующего законодательства. К данному выводу учёные пришли в результате детального исследования сложных вопросов квалификации преступлений против собственности в условиях цифровой трансформации [18, с.262]. Результаты данного исследования позволяют сделать вывод о том, что одной из основных сложностей изучения уголовных дел о преступлениях обозначенной специфики, поступивших для утверждения обвинительного заключения (акта, постановления), является проверка правильности квалификации действий обвиняемых. В связи с этим, в условиях неопределённости и наличия противоречивой судебной практики прокурору надлежит ориентироваться на научные работы в области уголовного права, которые посвящены вопросам квалификации киберпреступлений.

Таким образом, мы считаем, что эффективность современного прокурорского надзора за исполнением законов органами дознания и предварительного следствия при расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий, может быть повышена за счет его комплексного характера, акцентирования внимания в его организации и осуществлении на выявленных ключевых аспектах.

Прокурор при изучении материалов таких уголовных дел должен опираться не только на нормативные правовые акты, следственную и судебную практику, но и на научные практикоориентированные работы в области криминалистики, теории оперативно-розыскной деятельности, уголовного права, уголовного процесса, информатики и др.

Библиография

1. Организация и осуществление прокурорского надзора за процессуальной деятельностью органов дознания и органов предварительного следствия: учебник / науч. ред.: А.Г. Халиулин, Л.А. Щербич. – М.: ИД "Городец", 2024. – 416 с.
2. Головин, А. Ю. Криминалистические методы преодоления противодействия расследованию транспортных преступлений / А. Ю. Головин, О. П. Грибунов, А. А. Бибиков. – Иркутск: Восточно-Сибирский институт МВД РФ, 2015. – 164 с. EDN: VDJCNB
3. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: монография / В. Б. Вехов; Федеральное государственное образовательное учреждение высшего профессионального образования "Волгоградская академия Министерства внутренних дел Российской Федерации". – Волгоград: Волгоградская академия МВД России, 2008. – 401 с. EDN: QQQEDJ

4. Волеводз, А. Г. Следы преступлений, совершенных в компьютерных сетях // Российский следователь. 2002. № 1. С. 4-12. EDN: TBOGQD
5. Цифровая криминалистика: учебник для вузов / В. Б. Вехов [и др.]; под ред. В. Б. Вехова, С. В. Зуева. 2-е изд., перераб. и доп. – Москва: Издательство Юрайт, 2024. – 490 с.
6. Россинская, Е. Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе: монография / Е. Р. Россинская. – 4-е изд., перераб. и доп. – Москва: Норма : ИНФРА-М, 2025. – 576 с.
7. Оперативно-розыскная деятельность в цифровом мире: сборник научных трудов / под ред. доктора юридических наук, заслуженного юриста Российской Федерации В. С. Овчинского. – Москва: Издательский Дом "Инфра-М", 2021. – 630 с.
8. Информационные технологии в уголовно-правовой сфере: монография / под ред. А. И. Бастрыкина, А. Н. Савенкова. – М.: ЮНИТИ-ДАНА, 2023. – 279 с.
9. Архипова, Н. А., Кругликова, О. В., Шебалин, А. В., Янгаева, М. О. Расследование хищений, совершенных с использованием информационно-телекоммуникационных технологий. – Барнаул: Федеральное государственное казенное образовательное учреждение высшего профессионального образования "Барнаульский юридический институт Министерства внутренних дел Российской Федерации", 2023. – 91 с. EDN: RHVTFT
10. Рогова, Е. В. Уголовно-правовое противодействие киберпреступности в России и Китае: сравнительно-правовой аспект / Е. В. Рогова // Вестник Университета прокуратуры Российской Федерации. – 2024. – № 1(99). – С. 84-90. EDN: RMWIGB
11. Клевцов, К. К. Международное сотрудничество в борьбе с киберпреступностью в контексте противодействия новым вызовам и угрозам / К. К. Клевцов // Вестник Санкт-Петербургского университета. – 2022. – Т. 13, Вып. 3. – С. 678-695.
12. Тисен, О. Н. Особенности доказывания преступлений, связанных с легализацией (отмыванием) доходов, полученных преступным путем / О. Н. Тисен; Международный учебно-методический центр финансового мониторинга. – Москва: Общество с ограниченной ответственностью "Издательство Юнити-Дана", 2022. – 311 с. EDN: POSDIZ
13. Васюков, В. Ф., Волеводз, А. Г., Клевцов, К. К. Противодействие криптовалютным преступлениям в зарубежных странах. – Москва: ООО Издательский дом "Юрлитинформ", 2025. – 504 с. EDN: GKXXWS
14. Долгиева, М. М. Общественная опасность отмывания криптовалюты // Законность. – 2022. – № 6. – С. 35-38. EDN: UIZNWU
15. Безенков, И. А. Международный опыт противодействия коррупционным правонарушениям, совершаемым с использованием цифровой валюты // Законность. – 2024. – № 4. – С. 44-48. EDN: UOFPPI
16. Россинская, Е. Р., Сааков, Т. А. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров // Криминалистика: вчера, сегодня, завтра. – 2020. – № 3 (15). – С. 106-123. DOI: 10.24411/2587-9820-2020-10060 EDN: YKCUUH
17. Смирнов, А. В. Электронные доказательства, электронное доказывание, искусственный интеллект: что далее? / А. В. Смирнов // Уголовное судопроизводство. – 2024. – № 1. – С. 24-31. DOI: 10.18572/2072-4411-2024-2-24-31 EDN: LMDTVO
18. Рогова, Е. В., Перетолчин, А. П. Преступления против собственности в условиях цифровой трансформации / Е. В. Рогова, А. П. Перетолчин // Академический юридический журнал. – 2022. – Т. 23, № 3(89). – С. 256-264. DOI: 10.17150/1819-0928.2022.23(3).256-264 EDN: FLUEGA

Результаты процедуры рецензирования статьи

Рецензия выполнена специалистами Национального Института Научного Рецензирования по заказу ООО "НБ-Медиа".
В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов можно ознакомиться здесь.

Данная статья посвящена исключительно актуальной и практически значимой проблеме совершенствования прокурорского надзора в условиях цифровой трансформации преступности. Автор демонстрирует глубокое понимание предмета исследования, что выражается в комплексном анализе как теоретических, так и прикладных аспектов прокурорской деятельности при надзоре за расследованием киберпреступлений. Особую ценность работе придает опора на статистические данные МВД России, свидетельствующие о критически низкой раскрываемости преступлений данной категории (28,9%), что объективно доказывает необходимость переосмысления существующих подходов к прокурорскому надзору.

Методологическая основа исследования заслуживает высокой оценки: автор последовательно применяет системный анализ, рассматривая прокурорский надзор как многоаспектную деятельность, требующую интеграции знаний из различных отраслей права и смежных наук. Однако структурная организация материала представляет собой серьезный недостаток работы. Сплошной текст без тематических подзаголовков существенно затрудняет восприятие сложного материала и не соответствует стандартам научных публикаций. Отсутствие четкого разделения на такие логические блоки, как «Криминалистические аспекты прокурорского надзора», «Оперативно-розыскная деятельность в киберпространстве», «Международное сотрудничество» или «Финансовый мониторинг и криптовалюты», снижает системность изложения и делает навигацию по тексту практически невозможной.

Актуальность исследования не вызывает сомнений. Цифровизация преступной деятельности требует адекватного ответа со стороны правоохранительной системы, и прокурорский надзор играет в этом процессе ключевую роль. Автор убедительно доказывает, что традиционные подходы к надзору за расследованием преступлений устарели и не соответствуют вызовам времени, особенно в контексте трансграничного характера киберпреступности и использования криптовалют. Однако структурные недостатки мешают полному раскрытию потенциала исследования, поскольку важные практические рекомендации «теряются» в едином текстовом массиве.

Научная новизна проявляется в предложении комплексной модели прокурорского надзора, основанной на интеграции специальных знаний из области цифровой криминалистики, теории оперативно-розыскной деятельности, международного сотрудничества и финансового мониторинга. Особого внимания заслуживает анализ новейших инструментов расследования, таких как технология OSINT и система «Прозрачный блокчейн». Тем не менее, отсутствие структурного деления материала приводит к тому, что эти инновационные аспекты не получают должного акцента и визуального выделения в тексте.

Стиль изложения отличается профессиональной зрелостью и точностью формулировок, что соответствует уровню научной публикации. Однако плотность и насыщенность материала без четкого структурного деления создает когнитивную перегрузку для читателя. Введение подзаголовков позволило бы не только улучшить восприятие, но и

усилить логические связи между различными аспектами исследования.

Библиографический аппарат репрезентативен и включает актуальные источники, однако отсутствие структуры статьи затрудняет соотнесение конкретных источников с соответствующими разделами исследования. Это снижает эффективность использования библиографии как инструмента научного аппарата.

Практическая значимость работы исключительно высока, но структурные недостатки ограничивают ее потенциал. Четкое разделение на тематические блоки позволило бы трансформировать статью в практическое руководство для прокурорских работников. В существующем виде ценные рекомендации рассредоточены по тексту, что затрудняет их оперативное использование в практической деятельности.

В целом автор демонстрирует высокий уровень профессиональной компетентности и глубокое понимание проблематики, что делает статью ценным вкладом в развитие теории и практики прокурорского надзора в условиях цифровизации. Несмотря на отмеченные структурные недостатки, статья представляет собой качественное исследование, сочетающее теоретическую глубину с практической направленностью. После структурной оптимизации и введения тематических подзаголовков работа может быть рекомендована к публикации. Рекомендуется также дополнить библиографию работами следующих авторов: А.В. Шабалина (киберкриминалистика), В.А. Волеводза (международное сотрудничество), А.В. Смирнова (цифровые доказательства), а также актуальными публикациями в журналах "Законность" и "Уголовный процесс" за 2024-2025 годы, посвященными прокурорскому надзору в цифровой среде.

Результаты процедуры повторного рецензирования статьи

Рецензия выполнена специалистами Национального Института Научного Рецензирования по заказу ООО "НБ-Медиа".
В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов можно ознакомиться здесь.

Предметом исследования является прокурорский надзор за процессуальной деятельностью органов дознания и предварительного следствия по конкретной категории уголовных дел – о преступлениях, совершённых с использованием информационно-телекоммуникационных технологий. Автор не ограничивается общими положениями о надзоре, а фокусируется на выявлении и анализе ключевых, наиболее проблемных аспектов этой деятельности. Это позволяет сузить объект исследования до конкретных, практико-ориентированных рамок.
Методологическая основа статьи не выделяется в отдельный раздел исследования, но фактически является комплексной. Автор применяет статистический метод (актуальные оперативные данные МВД России); сравнительно-правовой метод (при анализе международного сотрудничества и новых конвенций); формально-юридический метод (для анализа норм уголовно-процессуального законодательства, ведомственных приказов Генпрокуратуры РФ); метод системного анализа (рассмотрение прокурорского надзора как многоаспектной деятельности); метод моделирования (косвенно автор предлагает модель построения эффективного прокурорского надзора).

Актуальность статьи обоснована автором, в том числе, с помощью статистических данных. Цифровая трансформация преступности и, как следствие, необходимость адаптации к ней всех субъектов правоохранительной системы, включая прокуратуру, делают исследование востребованным.

Научная новизна заключается в комплексном структурировании проблемы. В то время как многие ученые исследуют отдельно криминалистику киберпреступлений или прокурорский надзор вообще, автор предпринимает успешную попытку синтезировать эти направления применительно к надзорной деятельности прокурора. Новизна проявляется в четком выделении шести ключевых аспектов надзора (криминалистический, оперативно-розыскная деятельность, международное сотрудничество, финансовый мониторинг, уголовно-процессуальный, уголовно-правовой); аргументированном утверждении, что без интеграции специальных знаний из смежных научных областей надзор не может быть эффективным; актуализации темы с учетом новаций (Конвенция ООН против киберпреступности 2024 г. и др.).

Стиль статьи соответствует стилю научной публикации. Структура работы логична и последовательна: от общего обоснования проблемы к детальному разбору каждого аспекта и обобщающему выводу. Содержание отличается глубиной проработки. Каждый раздел подкреплен ссылками на авторитетные научные источники, ведомственные акты и современную практику. Особого внимания заслуживают практические примеры.

Список литературы соответствует теме исследования и включает 18 источников, значительная часть из которых опубликована в последние годы (2023-2025 гг.), что говорит о том, что автор оперирует актуальными научными данными.

Автор косвенно апеллирует к потенциальным оппонентам, которые могут считать традиционный подход к прокурорскому надзору достаточным. Он последовательно доказывает обратное, показывая, что стандартного знания УПК РФ и ведомственных инструкций сегодня недостаточно. Основной тезис, который может вызвать дискуссию – это требование к прокурору обладать широким спектром специальных знаний. Оппоненты могут указать на невозможность столь глубокой специализации в рамках одной должности, однако автор предвосхищает это возражение, говоря о необходимости «минимальных знаний» и о неизбежности развития цифровых компетенций в ближайшем будущем.

Вывод статьи логически вытекает из всего изложенного: эффективность надзора может быть повышена за счет его комплексного характера и акцента на выявленных ключевых аспектах. Статья адресована не только ученым-правоведам и преподавателям, но и практикам – прокурорам, следователям, дознавателям, сотрудникам оперативных подразделений.

Статья является самостоятельным, оригинальным научным исследованием, обладающим значительной научной и практической ценностью, и рекомендована к публикации.