ФГАОУ ВО «Балтийский федеральный университет
имени Иммануила Канта»

На правах рукописи

Орешков Иван Андреевич

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ЭКОНОМИКИ

Специальность 5.1.4. Уголовно-правовые науки

Диссертация
на соискание ученой степени кандидата юридических наук

Научный руководитель:
доктор юридических наук, профессор,
Заслуженный работник высшей школы РФ
Волчецкая Татьяна Станиславовна

Калининград
2026

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. Современные информационные технологии в последнее время все активнее внедряются в различные сферы общественной жизни. В настоящее время сложно представить специалиста, деятельность которого не была бы связана с их использованием в профессиональной деятельности.

Исключением в данном контексте не является и уголовное судопроизводство. Внедрение цифровых технологий в уголовное судопроизводство позволяет оптимизировать процесс расследования и последующего рассмотрения дел судами, повышает эффективность указанной деятельности, экономя при этом как временные, так и финансовые затраты. Кроме того, постепенно осуществляется переход от бумажного ведения делопроизводства к электронному.

По данным портала ЕМИСС, за январь-октябрь 2025 года в Российской Федерации зарегистрировано 95 538 преступлений экономической направленности, что уже более чем на 500 преступлений превышает аналогичный период 2024 года и более чем на 1000 преступлений аналогичный период 2023 года[1], что свидетельствует о росте количества этих преступлений. При этом специфика экономической деятельности в современной России, а именно масштабная цифровизация говорит о том, что расчеты между организациями производятся безналичным способом, контракты и договоры между предприятиями, а также между государственными органами и предприятиями заключаются на электронных площадках, закупки с целью обеспечения государственных и муниципальных нужд проводятся посредством электронного конкурса. Именно это и служит причиной использования информационно-

[1] Количество преступлений экономической направленности, зарегистрированных в отчетном периоде. Единая межведомственная информационно-статистическая система (ЕМИСС) [Электронный ресурс]. URL: https://www.fedstat.ru/indicator/36222 (дата обращения: 19.10.2025).

коммуникационных технологий при расследовании преступлений в сфере экономики.

Применение современных информационных технологий при расследовании преступлений в сфере экономики является необходимостью, обусловленной цифровизацией самой экономической деятельности и соответствующим развитием преступных схем. Эти преступления часто характеризуются большими объемами электронных данных, сложностью финансовых транзакций, анонимностью и трансграничностью, что делает традиционные методы расследования крайне неэффективными.

При анализе информации, сохраненной на электронных носителях (финансовых документов, документов бухгалтерского учета, договоров и их проектов, личных записей, хранящихся в электронном виде, а также при анализе электронной переписки между фигурантами, выписок о движениях денежных средств по расчетным счетам, истории соединения между абонентами и абонентскими устройствами, данных об IP-адресах, хранящихся у сетевых провайдеров и интернет-провайдеров), можно получить значительное количество доказательственной информации, подтверждающей как образование умысла, так и доказывающих механизм совершения преступления. В силу этого тема диссертационного исследования является актуальной и практически значимой.

Степень разработанности проблемы. Анализируемые проблемы вызывали и вызывают научный интерес прежде всего у ученых в области уголовного процесса и криминалистики.

Изучению проблем расследования преступлений в сфере экономики посвящены работы таких видных ученых-криминалистов, как И. В. Александров, Л. В. Бертовский, А. В. Варданян, А. Ф.Волынский, Ю. В. Гаврилин, С.Ю. Журавлев, И.В. Ильин, А.Ф. Лубин, Н.В. Макарейко, А.А. Модогоев, Е.В. Чиненов, Л.Г. Шапиро и других авторов.

Проблемы информационного обеспечения раскрытия и расследования преступлений, а также использования современных информационных технологий

в уголовном производстве подробно описаны в трудах известных ученых, таких как Л.В. Бертовский, А.В. Булыжкин, А.В. Варданян, В. Ф. Васюков, В.Б. Вехов, Ю.В. Гаврилин, Г.А. Гундерич, Е.П. Ищенко, Е. А. Комаров, А.Н. Колычева, Т.Е. Кузнецов, И.А. Макаренко, В. А. Мещеряков, В.С. Овчинский, А.Л. Осипенко, А.В. Победкин, С. Б. Россинский, Е.Р. Россинская, П.Г. Смагин, В.Ю. Стельмах, Д. А. Степаненко и других.

Основы методики расследования преступлений с применением информационно-коммуникационных технологий и компьютерной информации представлены в диссертационном исследовании В.А. Мещерякова (2001). Отдельным проблемам развития российского уголовного судопроизводства в условиях цифровизации посвящены труды А. С. Александрова, О. И. Андрее-вой, О.А. Зайцева, Х.Х. Рамалданова, Ю.Н. Соколова.

Вопросы применения искусственного интеллекта в качестве вспомогательного средства при расследовании уголовных дел раскрыты в работах Л.В. Бертовского, А.А. Бессонова, С.В. Зуева, А.Ю. Головина и других. Исследованиям, посвященным ситуационным особенностям расследования преступлений с использованием современных информационных технологий, посвящены труды Д.В. Бахтеева, Т.С. Волчецкой, С.И. Давыдова, Л. Я. Драпкина, В.Н. Карагодина, Д.В. Кима, А.С. Князькова, Н.П. Яблокова и других авторов.

Важность научных трудов названных авторов для юридической науки неоспорима, вместе с тем отметим, что в настоящее время отсутствуют научные исследования, в которых изучаются проблемы применения современных информационных технологий при расследовании преступлений в сфере экономики

Объектом исследования стала деятельность следователя по расследованию преступлений в сфере экономики с использованием современных информационных технологий.

Предметом диссертационного исследования являются закономерности деятельности правоохранительных органов по выявлению, изучению и

использованию в доказывании следов преступлений в сфере экономики, совершенных с применением современных информационных технологий.

Цель диссертационного исследования заключается в разработке теоретических положений и практических рекомендаций по использованию различных видов информационных технологий при расследовании преступлений в сфере экономики.

Достижение поставленной цели обусловило необходимость решения следующих **задач**:

1. Сформулировать понятие, раскрыть особенности и виды современных информационных цифровых и информационно-коммуникационных технологий, применяемых в уголовном судопроизводстве.

2. Выделить основные направления использования современных информационных технологий при расследовании преступлений в сфере экономики.

3. Раскрыть криминалистические особенности преступлений в сфере экономики, обусловливающие необходимость применения современных информационных технологий при их расследовании.

4. Выявить проблемы правовой регламентации и разработать алгоритм использования информационных технологий для фиксации следовой картины преступлений в сфере экономики.

5. Раскрыть тактические особенности проведения допросов с применением видео-конференц-связи, разработать тактические приемы таких допросов, проводимых при расследовании преступлений в сфере экономики.

6. Выявить проблемы изъятия и осмотра электронных носителей информации, возникающие при расследовании преступлений в сфере экономики, и предложить научно обоснованные пути решения указанных проблем.

7. Определить проблемы получения электронной информации о переписках у операторов и провайдеров, выявить их процессуальные и тактические особенности, разработать научно обоснованные рекомендации.

8. Выявить специфику использования специальных знаний при расследовании преступлений в сфере экономики, совершенных с использованием информационных технологий.

Методологической основой данного диссертационного исследования послужили *общенаучные и частные методы*, разработанные в криминалистике. В их число вошли такие *методы*, как *анализ, синтез, индукция, дедукция, аналогия* и *обобщение. Системно-структурный* метод и метод *моделирования* применялись для определения структуры и элементов механизма совершения экономических преступлений. Благодаря *системному подходу* удалось установить характерные особенности механизма следообразования в этой сфере, включая электронные следы, что позволило четче обозначить объект исследования. *Статистический метод* оказался незаменим для анализа и обобщения эмпирических данных о практике расследования преступлений в сфере экономики, совершаемых с применением информационных технологий. *Сравнительно-правовой метод* использовался для анализа норм отечественного уголовно-процессуального права, регулирующих применение информационных средств фиксации следов (включая видео-конференц-связь), и сравнения их с нормами государств-членов СНГ. Наконец, ситуационный подход позволил разработать научно обоснованные рекомендации по применению информационных технологий в различных следственных ситуациях, возникающих при расследовании преступлений в сфере экономики.

Нормативно-правовую базу исследования составили Конституция Российской Федерации, Уголовный кодекс Российской Федерации, Уголовно-процессуальный кодекс Российской Федерации, Федеральный закон «Об оперативно-розыскной деятельности», Федеральный закон «Об информации, информационных технологиях и о защите информации», Федеральный закон «О государственной судебно-экспертной деятельности в Российской Федерации» и иные федеральные законы.

Теоретической основой диссертации послужили труды известных криминалистов: Р. С. Белкина, Л. В. Бертовского, А. А. Бессонова, Н. И. Валькирии (Малыхиной), А.В. Варданяна, В.Ф. Васюкова, В.Б. Вехова, А. Г. Волеводза, Т. С. Волчецкой, Ю. В. Гаврилина, Ю. П. Гармаева, А. Ю. Головина, О. П. Грибунова, А. Н. Григорьева, С. И. Давыдова, Л. Я. Драпкина, Е. С. Дубоносова, С. Ю. Журавлева, С. В. Зуева, Е. П. Ищенко, Д. В. Кима, А. С. Князькова, Н. П. Майлис, И. А. Макаренко, В. А. Мещерякова, В. С. Овчинского, А. Л. Осипенко, Н. А. Подольного, С. Б. Россинского, Е. Р. Россинской, Е. В. Смахтина, Д. А. Степаненко, Т. В. Толстухиной, Е. В. Чиненова, Л. Г. Шапиро, Е.Н. Холоповой, Н.П. Яблокова и других авторов.

Эмпирическую основу исследования составили данные, полученные в результате изучения материалов 122 уголовных дел, рассмотренных судами Москвы, Санкт-Петербурга, Московской, Ленинградской, Калининградской, Новгородской, Ростовской, Архангельской областей, Краснодарского края, за период с 2012 по 2025 год; а также результаты исследования статистических данных, размещенных на официальном интернет-сайте Судебного департамента при Верховном Суде Российской Федерации за период с 2014 по 2024 год.

Эмпирической базой работы также стали результаты интервьюирования 107 практических работников, в их числе 68 следователей подразделений МВД России и 39 следователей Следственного комитета Российской Федерации Московской, Ленинградской, Мурманской, Сахалинской, Свердловской, Ростовской, Калининградской, Новгородской, Псковской областей, Краснодарского края, Республики Коми, Москвы и Санкт-Петербурга. При проведении исследования использовался и личный практический опыт работы автора, проходившего службу в должности следователя в следственных подразделениях МВД России и в органах прокуратуры.

Научная новизна исследования заключается в том, что на основе системного, междисциплинарного и ситуационного подходов автором на монографическом уровне разработаны теоретические основы использования

информационных технологий при расследовании преступлений в сфере экономики, выявлены проблемы применения информационных технологий при расследовании вышеуказанных преступлений и предложены пути их решения.

Научная новизна диссертации заключается также в том, что в ней:

– уточнены понятия информационных, цифровых и информационно-коммуникационных технологий, используемых в уголовном судопроизводстве, показана необходимость их дифференциации;

– выделены основные направления и виды применения информационных технологий при расследовании преступлений в сфере экономики;

– выявлены криминалистические особенности преступлений в сфере экономики, обусловливающие необходимость широкого использования информационных технологий при их расследовании;

– разработан алгоритм применения информационных технологий, предназначенных для фиксации следовой картины преступлений, совершенных в сфере экономики, выявлены проблемы правовой регламентации использования таких средств и предложены пути их решения;

– с криминалистических позиций обоснована нецелесообразность законодательного закрепления обязательности привлечения понятых к участию в следственных действиях, связанных с копированием информации с электронных носителей, а также специалиста к участию в следственных действиях, связанных с изъятием электронных носителей информации либо копированием с них электронной доказательственной информации;

– разработаны ситуационно обусловленные тактические приемы и рекомендации по применению современных информационных технологий в процессе проведения допросов с использованием видео-конференц-связи;

– выявлены проблемы изъятия электронных носителей информации при расследовании преступлений в сфере экономики, а также проблемы получения электронной информации о переписках у операторов и провайдеров, предложены пути их разрешения;

– разработаны тактические рекомендации фиксации электронных следов в ситуациях, когда искомая информация сохранена в облачных хранилищах;

– предложены тактические рекомендации по проведению осмотра электронных носителей информации;

– установлена специфика использования специальных знаний при расследовании преступлений в сфере экономики, совершенных с применением информационных технологий, разработаны научно обоснованные рекомендации по расширению использования современных информационных технологий в экспертной практике.

Основные положения, выносимые на защиту:

1. Уточнены понятия информационных, цифровых и информационно-коммуникационных технологий, применяемых в уголовном судопроизводстве, показана необходимость их дифференциации. Информационные технологии – более широкое понятие, под которым в криминалистическом аспекте предлагается понимать технологии, используемые в процессе собирания, обработки, накопления и передачи криминалистически значимой информации, при функционировании которых происходит образование информации нового качества о состоянии объекта, процесса или явления. Цифровые технологии и информационно-коммуникационные технологии являются подвидами информационных технологий. Так, цифровые технологии – это технологии, использующие совокупность средств и методов собирания, обработки, накопления и передачи криминалистически значимой информации сбора, обработки, накопления и передачи данных (первичной информации) для получения информации нового качества о состоянии объектов, процессов, явлений с применением цифрового (двоичного) кода. При этом информационно-коммуникационные технологии – это инфраструктура передачи данных по ее каналам и связанная с ней обработка информации. Дифференциация указанных понятий необходима с целью унификации языка криминалистики и

единообразного подхода к разработке научно обоснованных криминалистических рекомендаций.

2. Выделены основные виды информационных технологий, используемых при расследовании преступлений в сфере экономики:

– информационно-справочные и аналитические системы;

– системы электронного документооборота и управления следственным процессом;

– информационные технологии, предназначенные для поиска и фиксации криминалистически значимой информации;

– информационные технологии, применяемые для коммуникации и дистанционного взаимодействия.

3. Выделены основные направления использования информационных технологий в следственной практике:

– использование информационно-справочных и аналитических систем для поиска информации;

– использование информационных технологий, предназначенных для фиксации следовой картины преступлений (средства сбора, фиксации и исследования доказательств);

– использование информационных технологий для коммуникации и дистанционного взаимодействия;

– использование технологий для организации предварительного следствия (программные комплексы для ведения электронного дела, использование синхронных переводчиков, нейросетей);

– использование технологий систем для электронного документооборота и управления следственным процессом.

4. Выявлены криминалистические особенности преступлений в сфере экономики, обусловливающие необходимость применения информационных технологий при их расследовании. Предметом преступного посягательства по таким преступлениям на современном этапе являются денежные средства,

ценные бумаги, имущественные права, иное имущество, имеющие документарную форму выражения, представленную в цифровом виде. Основные действия, характеризующие способ совершения указанных преступлений, происходят удаленно и дистанционно с доступом в сеть Интернет, в том числе посредством интернет-банкинга для совершения платежей. Анализ следовой картины современных преступлений в сфере экономики преступлений позволил выявить преобладание «электронных» следов среди иных материальных.

5. С криминалистических позиций обоснована нецелесообразность законодательного закрепления обязательности привлечения понятых к участию в следственных действиях, связанных с копированием информации с электронных носителей, а также специалиста к участию в следственных действиях, связанных с изъятием электронных носителей информации либо копированием с них электронной доказательственной информации. Это обусловлено тем, что сведения о скопированной информации, а именно о времени, дате, устройстве, с которого была скопирована информация, уже автоматически отображаются в свойствах скопированного файла.

Участие специалиста в следственных действиях по изъятию электронных носителей и копирования с них информации обусловлено ситуационной необходимостью: в ситуациях изъятия электронных носителей информации, не являющихся технически сложными (смартфоны, ноутбуки, USB-флеш-накопители и др.), компетенции следователя вполне достаточно для их самостоятельного изъятия.

С целью оптимизации следственной и экспертной деятельности и экономии кадровых ресурсов предложено исключить из ч. 2 ст. 164.1 УПК РФ требование об обязательном участии понятых и специалиста в ходе изъятия электронных носителей и копирования с них информации.

6. Разработаны научно обоснованные рекомендации по алгоритмизации первоначальных следственных действий при расследовании преступлений в

сфере экономики, ситуационная обусловленность которых требует получения электронной доказательственной информации.

Первоначально необходимо определить круг лиц (технических устройств, абонентских номеров, электронных почтовых ящиков, аккаунтов в мессенджерах), где может быть обнаружена криминалистически значимая информация. Второй шаг – проведение обысков и выемок с целью изъятия электронных носителей информации у их владельцев. Далее следует провести выемки в организациях, обеспечивающих передачу сообщений/звонков по сетям электросвязи электронных переписок. Данная выемка обеспечит установление удаленных сообщений, хранящихся на серверах соответствующей организации, которые не будут обнаружены в ходе осмотра электронных носителей информации. После чего необходимо истребовать детализации о соединениях между абонентами и абонентскими устройствами, а также выписки по расчетным счетам организаций и граждан, ставших фигурантами преступлений.

7. Аргументирована целесообразность и разработаны тактические приемы проведения допросов посредством использования видео-конференц-связи из-за невозможности явки лица, проживающего на значительном отдалении от органа предварительного следствия, в следственный орган по месту его жительства с использованием электронно-цифровой подписи. Рекомендован дистанционный вариант участия таких лиц с использованием в качестве электронно-цифровой подписи функций приложения «Госключ». Предложены тактические рекомендации по проведению допросов с использованием видео-конференц-связи, включая особенности расположения участвующих лиц в кадре при видеосъемке следственного действия и возможности криминалистического наблюдения за их поведением.

8. Разработаны тактические рекомендации фиксации электронных следов в ситуациях, когда искомая информация сохранена в облачных хранилищах, с помощью их фиксации фотографированием, видеосъемкой или копированием данных.

Предложены тактические рекомендации по проведению осмотра электронных носителей информации. Акцентировано внимание на необходимость проведения осмотра согласно предложенному алгоритму действий.

При наличии риска утраты доказательственной информации при включении мобильных устройств, в том числе, в которых функционально предусмотрено использование e-sim, необходимо привлекать к участию в следственном действии специалиста, обладающего специальными познаниями в области радиотехники с целью применения им специальных устройств, предназначенных для подавления связи для предотвращения удаления или искажения данных.

По результатам криминалистического анализа проблем изъятия и осмотра электронных носителей информации предложено дополнить статью ч. 1 ст. 164.1 УПК РФ пунктом 4, в который следует включить новое основание, позволяющее изымать такие носители: «если копирование данных невозможно по техническим причинам при наличии соответствующего заявления специалиста, участвующего в следственном действии».

Вместе с тем для предотвращения неправомерного применения мер, которые могут воспрепятствовать обеспечению законных прав и интересов граждан и законной деятельности организаций и предпринимателей, предложено установить сроки для осмотра таких носителей, их признания вещественными доказательствами, а также для назначения экспертизы по аналогии с общим сроком осмотра электронных носителей информации при расследовании преступлений экономической направленности, закрепленном в ч. 2 ст. 81.1 УПК РФ (10 суток, который может быть единожды продлен по мотивированному ходатайству до 30 суток).

9. Разработаны тактические приемы выемки электронных сообщений в учреждениях, предоставляющих услуги их передачи через сеть Интернет. Предложено проводить изъятие как существующих на электронном почтовом

ящике писем, так и тех электронных сообщений, которые были удалены; запрашивать информацию о регистрационных данных, которые пользователи указывали при создании аккаунта; подавать ходатайство в суд о разрешении проведения следственного действия на первоначальном этапе расследования с целью предотвращения возможной утраты следов преступления. В отдельных случаях предложено проводить изъятие электронных сообщений, хранящихся на серверах организаций с помощью их «перемещения», а не общепринятого «копирования».

10. Доказана необходимость оптимизации использования специальных знаний при расследовании преступлений в сфере экономики путем широкого внедрения в деятельность эксперта и специалиста информационных технологий. Для решения проблемы эффективного извлечения и анализа больших объемов данных, необходимо совершенствование аппаратно-программных комплексов, применяемых специалистами и экспертами при проведении исследований. Требуется создание новых методик проведения исследований и экспертиз исходя из развития технологий и современных платежных систем и систем бухгалтерского учета. Для автоматизации рутинных операций целесообразна разработка программ по использованию искусственного интеллекта и машинного обучения. Исходя из этого, требуется внедрение междисциплинарных образовательных программ для экспертов, объединяющих знания в области юриспруденции, экономики, бухгалтерского учета и современных информационных технологий.

Теоретическая значимость исследования заключается в том, что сформулированные в нем выводы и положения, а также результаты исследования проблемных вопросов расследования преступлений, совершенных в сфере экономики с применением современных информационных технологий, обогащают научные положения в области криминалистической техники, тактики и методиках расследования отдельных видов преступлений.

Практическая значимость определяется возможностью применения полученных результатов исследования для оптимизации деятельности по расследованию и профилактике преступлений в сфере экономики. Отдельные выводы исследования могут использоваться:

– в практической деятельности органов предварительного расследования при раскрытии, расследовании и предупреждении преступлений в сфере экономики;

– в экспертной практике;

– в учебном процессе образовательных учреждений юридического профиля;

– при повышении квалификации следователей, дознавателей, прокуроров и оперативных сотрудников.

Апробация и внедрение результатов исследования. Основные результаты исследования докладывались и обсуждались на международных, всероссийских и региональных научно-практических конференциях, проходивших в Балтийском федеральном университете имени И. Канта (2023, 2024, 2025), Уральском государственном университете им. В.Ф. Яковлева (2023), Национальном исследовательском университете «Московский институт электронной техники» **(**2023), Российском государственном университете правосудия (2022, 2023), Карагандинском университете Казпотребсоюза (Казахстан) (2022, 2023).

Основные результаты и выводы диссертационного исследования нашли отражение в 10 опубликованных работах автора, 4 из которых опубликованы в изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации.

Положения диссертации обсуждались на заседаниях экспертного совета по специальности 5.1.4. Уголовно-правовые науки Высшей школы права БФУ им. И. Канта.

Результаты диссертационного исследования внедрены в практическую деятельность СУ УМВД России по Калининградской области, Калининградского следственного отдела на транспорте Западного межрегионального Следственного управления на транспорте СК России.

Отдельные положения диссертационного исследования были внедрены в учебный процесс Высшей школы права БФУ имени И. Канта.

Структура и объем диссертации. Диссертация состоит из введения, двух глав, включающих восемь параграфов, заключения, списка использованной литературы и приложений.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ЭКОНОМИКИ

1.1. Понятие, признаки и виды современных информационных технологий в уголовном судопроизводстве

Для того чтобы рассмотреть особенности применения информационных технологий при расследовании преступлений в сфере экономики, необходимо исследовать понятие, сущность таких технологий, и специфику их применения в уголовном судопроизводстве.

И в этом плане, в первую очередь, необходимо проанализировать терминологический аппарат, используемый сотрудниками правоохранительных органов, а также учеными, проводящими исследования в этой сфере[1]. Анализ научной литературы, а также проведенное нами интервьюирование следователей позволило сделать вывод о том, что сегодня довольно широко используются такие термины как «информационные технологии» и «цифровые технологии». Причем в следственной практике они нередко используются как синонимы, а в науке некоторые авторы усматривают между ним и разницу, а некоторые – нет.

Вопросам внедрения информационных технологий в различные сферы деятельности человека посвящено большое количество научных трудов. Ввиду чего, анализируя определения, данные информационным технологиям различным учеными и авторами Р.В. Акоевой, А.П. Жуковым, А.А. Максутовым, а также анализируя законодательно закрепленное понятие информационных технологий, можно констатировать различия в формулировках, в некоторых случаях определение информационных технологий является

[1] См. об этом Светличный А.А. Криминалистическая терминология в теории и практике противодействия преступной деятельности: автореф. дис. ... канд. юрид. наук. Калининград, 2024. 53 с

довольно абстрактным, а в некоторых случаях наоборот излишне конкретизированным.

Кроме того, в контексте рассмотрения данных проблем, определения «информационные технологии» и «цифровые технологии» стали употребляться почти как равнозначные. Вместе с тем, содержания указанных понятий, на наш взгляд, имеют существенные различия, ввиду чего считать их синонимами представляется не совсем правильным.

Такой порядок использования терминологии, при котором в одни и те же понятия различными авторами вкладывается различный смысл, затрудняет как понимание содержания этих терминов в юридической литературе, так и затрудняет использование на практике следователями научных рекомендаций в ходе деятельности по расследованию преступлений.

Ввиду чего, в целях перехода к унифицированному языку права, основными признаками которого являются точность, ясность, использование слов и терминов в строго определенном смысле, представляется необходимым провести анализ понятий «информационные технологии», «информационно-коммуникационные технологии» и «цифровые технологии», а также выделить наиболее точную и понятную формулировку данных определений для их использования в науке.

В своих трудах Т.С. Волчецкая справедливо обращает внимание на необходимость унификации понятийного аппарата, используемого в научной литературе при описании проблем, связанных с использованием информационных технологий в криминалистике. В частности, по ее мнению, одним из необходимых направлений развития теории информационно-компьютерного обеспечения криминалистической деятельности является создание тезауруса, в котором должны быть закреплены основные понятия,

используемые в исследованиях, связанных с изучением цифровизации криминалистической науки.[1]

Определение понятия информационных технологий имеет как теоретическую, так и безусловную практическую значимость, применительно к юриспруденции, уголовному судопроизводству, а также к расследованию преступлений в сфере экономики. Теоретическая значимость выражается как в унификации языка права, так и систематизации, классификации и уточнении видов информационных технологий, правовых явлений, связанных с информационными технологиями, способствует правовой грамотности[2].

В свою очередь, практическая значимость данного понятия применительно к расследованию преступлений в сфере экономики связана с ее нормативным закреплением, в том числе законодательной техникой использования определения информационных технологий в нормативных актах; разработкой методик, связанных поиском и фиксацией следов преступлений, которые могут быть оставлены с использованием информационных технологий, а также зафиксированы с их помощью.[3]

---

[1] См. об этом: Волчецкая, Т. С. Развитие языка криминалистики в условиях цифровизации / Т. С. Волчецкая // Высокотехнологичное право: современные вызовы : Материалы IV Международной межвузовской научно- практической конференции, Москва-Красноярск, 17–20 февраля 2023 года. Том Часть 1. – Красноярск: Красноярский государственный аграрный университет, 2023. – С. 51-56. – EDN JFQPLE.

[2] См. подробнее: Светличный, А. А. Криминалистическая терминология в теории и практике противодействия преступной деятельности: автореф. дис ... д-ра юрид. наук : 5.1.4 / А. А. Светличный. – Тула: Тульский гос. ун-т, 2024. – 53 с.

[3] См. подробней: Жуков, А. П. Информационные технологии: уточнение понятия и нормативные основы правового регулирования / А. П. Жуков // Образование и право. – 2024. – № 12. – С. 434-438. – DOI 10.24412/2076-1503-2024-12-434-438. – EDN CNUMUF; Максуров, А. А. Особенности информационных технологий как правовой категории / А. А. Максуров // Вестник Юридического института МИИТ. – 2024. – № 3(47). – С. 53-60. – EDN JVDSEF; Акоева, Р. В. Информационные технологии в юридических исследованиях / Р. В. Акоева, В. Б. Сугарова // Научно-техническая конференция обучающихся и молодых ученых СКГМИ (ГТУ) "НТК-2017": сборник докладов по итогам научно-исследовательских работ, Владикавказ, 26–30 апреля 2017 года / Северо-Кавказский горно-металлургический институт (государственный технологический университет). – Владикавказ: Северо-Кавказский горно-металлургический институт (государственный технологический университет), 2017. – С. 25-26. – EDN YTOFCG.

Для определения содержания термина «информационные технологии» необходим семантический анализ самого понятия «информационные технологии». Как видно, указанное понятие складывается из двух слов – «информация» и «технология».

Согласно ГОСТ Р 52653_2006 «Информационно-коммуникационные технологии в образовании. Термины и определения» под информацией понимаются «сведения (сообщения, данные) независимо от формы их представления».[1]

Как известно, понятие «информация» имеет латинские корни, указанное определение произошло от латинского слова informatio, что означает сообщение, разъяснение, изложение.

Понятие информации, как справедливо отметили В.В. Степанов и А.Д. Урсул, является междисциплинарным, и пронизывает множество научных областей, от математики (теория информации Шеннона и Уивера) до биологии (генетика)[2]. А.Д. Урсул подчеркивает, что информационный подход, сочетающий теоретические идеи и математические инструменты, стал общенаучным методом[3]. Информация определяется по-разному: как сообщение, устранение неопределенности, сигнал, управляющий процесс, а также как отражение разнообразия в объектах и процессах.

Наряду с исследованием значения определения «информации», необходимо обратиться к понятию «технологии». Понимание термина "технология" (от греч. "techne" - искусство и "logos" - учение) эволюционировало. Советская энциклопедия 1987 года определяла технологию как совокупность методов обработки сырья и материалов в производстве, целью которой является

---

[1] "ГОСТ Р 52653-2006. Национальный стандарт Российской Федерации. Информационно-коммуникационные технологии в образовании. Термины и определения" (утв. и введен в действие Приказом Ростехрегулирования от 27.12.2006 N 419-ст).

[2] См. подробней: Степанов В.В. «От информационных технологий к информационным онтологиям» / Ученые записки Крымского федерального университета имени В. И. Вернадского. Социология. Педагогика. Психология, 2012

[3] См. об этом: Урсул А. Д. Проблема информации в современной науке/А. Д. Урсул . - 1975

выявление и применение наиболее эффективных процессов. Впервые термин ввел И. Бекман в 1772 году, описывая ремесленные навыки и знания. В XIX-XX веках "технология" чаще ассоциировалась с промышленностью, при этом часто использовался синоним "техника". В современной литературе "технология" преобладает, хотя иногда термин "technology" по-прежнему переводят как "техника".

По мнению В.А. Литовой, современные технологии — это не просто совокупность знаний и навыков для организации деятельности и выполнения определенных процедур[1]. По ее мнению, современные технологии представляют собой сложную иерархическую систему управления производственными процессами, направленную на их оптимизацию, модернизацию и постоянное инновационное развитие.

Проанализировав значения определений, являющихся составными частями понятия «информационные технологии», следует провести анализ указанного определения.

Согласно Федерального Закона «Об информации, информационных технологиях и о защите информации» № 149-ФЗ, под информационными технологиями понимаются «процессы, использующие совокупность средств и методов сбора, обработки, накопления и передачи данных (первичной информации) для получения информации нового качества о состоянии объекта, процесса, явления, информационного продукта, а также распространения информации и способы осуществления таких процессов и методов».[2]

[1] См. подробней: Литова В.А. «Сущность понятия "технология" на современном этапе» / Ученые записки. Электронный научный журнал Курского государственного университета, 2019

[2] Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 24.06.2025) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.09.2025).

Кроме того, понятие информационных технологий нормативно закреплено в ГОСТ 59853-2021[1], согласно которого под информационными технологиями также понимаются «приёмы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных».

В науке, как было сказано ранее, учеными выделяются также различные мнения относительно того, что следует понимать под информационными технологиями.

М.О Медведевой, С.Ю. Наточий, Г.И. Сафоновым, информационные технологии определяются как «интегрированная система методов, программного обеспечения и технических средств, обеспечивающая обработку, хранение, управление и представление информации для повышения оперативности, достоверности и удобства использования информационных ресурсов»[2].

По мнению В.С. Володченко, Д.С. Ланцовой, Т.А. Мироновой, информационные технологии можно широко определить как использование компьютеров, программного обеспечения (операционной системы, инструментов и приложений), коммуникаций и сетей для обеспечения удовлетворения информационных потребностей организации[3].

Информационные технологии (ИТ) представляют собой широкий класс дисциплин и областей деятельности, которые относятся к технологиям формирования и управления процессами работы с данными и информацией, с применением вычислительной, компьютерной и коммуникационной техники.

---

[1] Национальный стандарт РФ ГОСТ Р 59853-2021 "Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения" (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 19 ноября 2021 г. N 1520-ст).

[2] См.: Медведева М.О., Наточий С.Ю., Сафонов Г.И. «Понятие информационных технологий и их значение при расследовании преступлений» / «Вестник Московского Университета МВД России», М., 2021

[3] См. об этом: Володченко В.С., Ланцова Д.С., Миронова Т.А. «Понятие и классификация информационных технологий» / «Достижения науки и образования», 2020

Информационные технологии включают в себя все ресурсы, которые необходимы для управления информацией, в частности компьютеры, программное обеспечение и сети, необходимые для создания, хранения, управления, передачи и поиска информации.

Однако, по нашему мнению, вышеуказанная трактовка определения информационных технологий является узкой, поскольку не охватывает весь спектр процессов и аппаратных комплексов, с помощью которых совершаются операции с данными. Данное определение только на применении компьютерных технологий применительно к осуществлению текущей деятельности организаций, в то время как информационные технологии охватывают не только компьютерные технологии, но и иные технологии образования информации (к примеру, аналоговое телевидение, радиовещание, иные средства автоматизированного управления процессами, не связанного с компьютерными технологиями).

Н.В. Агеев полагает, что, информационные технологии служат важным инструментом в расследовании преступлений, оптимизируя поиск, сбор, хранение и обработку информации. Они повышают эффективность работы следователей, экспертов, оперативных сотрудников и судей, улучшая процессы принятия решений в рамках уголовного судопроизводства[1].

Наиболее емкое понятие информационных технологий представлено В.В. Степановым, который под информационными технологиями понимает «такие технологии, которые могут совершать следующие операции: ввод данных, специальная обработка с введенными данными, вывод данных»[2].

Также, по мнению В.В. Степанова, любая система, позволяющая кодировать и декодировать информацию, записывать и изменять её на носителе, и

[1] См. подробнее: Агеев Н.В. «Организация использования информационных технологий в расследовании» / «Гуманитарные, социально-экономические и общественные науки», 2022

[2] См. подробней: Степанов В.В. «От информационных технологий к информационным онтологиям» / Ученые записки Крымского федерального университета имени В. И. Вернадского. Социология. Педагогика. Психология, 2012

обрабатывать вводимые данные, может быть названа информационной технологией.

Анализируя с точки зрения криминалистики вышеуказанные определения информационных технологий, регламентированных в нормативных в нормативных актах и предложенных наукой, считаем, что наиболее емким и точным определением является следующее.

Информационные технологии - это технологии, используемые в процессе собирания, обработки, накопления и передачи криминалистически значимой информации, при функционировании которых происходит образование информации нового качества о состоянии объекта, процесса или явления.

Нельзя отождествлять информационные технологии с компьютерными, поскольку кроме них к числу информационных относятся и иные технологии, осуществляющие сбор, обработку, накопление и передачу данных, не применяя двоичную систему и иные значимые особенности компьютерных технологий, – как выше указывалось – это и аналоговое телевидение, радиовещание, иные средства автоматизированного управления процессами, не связанного с компьютерными технологиями.

Указанное определение по большей части соотносится с законодательным определением информационных технологий, поэтому в ходе исследования законодательное определение информационных технологий берется нами за основу.

Анализируя законодательные и научные определения информационных технологий, предполагающих такие технологические процессы как сбор, обработку, накопление и передачу данных, с учетом современного состояния цифровизации практически всех областей человеческой деятельности, можно сделать вывод, о том, что на современном этапе понятие информационных технологий не отделимо от использования в них вычислительной техники.

Как было упомянуто В.А. Литовой, технология на современном этапе в связи с развитием прогресса не отделима от инноваций. В связи с чем, на

современном этапе, современные информационные технологии не могут существовать раздельно от внедрения в них информационно-вычислительной техники[1].

В связи с чем, в настоящее время понятие информационных технологий в научной литературе зачастую стало охватывать и такие понятия как информационно-коммуникационные технологии и цифровые технологии.

Однако в целях унификации научной юридической терминологии, считаем необходимым остановиться на каждом из научных определений и проанализировать их содержание.

Законодательного понятия информационно-коммуникационных и цифровых технологий не имеется, вместе с тем проанализировав указанные определения, имеющиеся в научной литературе можно их сопоставить, какое из них является более общим, а какое является частью от целого.

Согласно определения информационно-коммуникационных технологий, представленного в ГОСТ Р 52653_2006 «Информационно-коммуникационные технологии в образовании», под информационно-коммуникационными технологиями понимаются информационные процессы и методы работы с информацией, осуществляемые с применением средств вычислительной техники и средств телекоммуникации[2].

Как указывает в своих трудах Д.В. Валько[3], информационно - коммуникационные технологии основаны исключительно на обмене информацией. Сам термин «коммуникация», имеющийся в данном словосочетании явно указывает на это. Информационно-коммуникационные технологии представляют собой инфраструктуру передачи данных и связанную с

---

[1] См. об этом: Литова В.А. «Сущность понятия "технология" на современном этапе» / Ученые записки. Электронный научный журнал Курского государственного университета, 2019

[2] ГОСТ Р 52653-2006 «Информационно-коммуникационные технологии в образовании. Термины и определения», утвержден Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 419-ст.

[3] См.: Валько Д.В. «Информационные технологии как вид экономической деятельности» / «Междисциплинарный диалог: современные тенденции в общественных, гуманитарных, естественных и технических науках», 2014

ней обработки информации. Обмен информацией производится по каналам её передачи. Компьютеры могут обмениваться информацией с использованием каналов связи различной физической природы: кабельных, оптоволоконных, радиоканалов и др.

Таким образом, понятие «информационно-коммуникационные технологии» является меньшим по объему, чем понятие «информационные технологии», так как само по себе оно определяет более узкий и конкретный объём инфраструктуры информационных технологий, который заключается именно в коммуникации – обмене информацией. Таким образом, информационно-коммуникационные технологии – это инфраструктура передачи данных по ее каналам и связанная с ней обработка информации.

Обращаясь к определению цифровых технологий, следует отметить, что в современной науке под цифровыми технологиями понимается система обработки информации, использующая эффективные методы кодирования и передачи данных[1]. Однако, специфичной особенностью именно цифровых технологий является то, что цифровые технологии основаны на цифровом представлении информации с использованием двоичного кода - с использованием нулей и единиц.

В отличие от аналоговых технологий, использующих непрерывные изменения сигналов (например, аналоговое телевидение или докомпьютерные системы автоматического управления), цифровые технологии оперируют дискретными значениями[2].

Из вышеизложенного можно сделать вывод о том, что понятие информационных технологий шире, чем цифровых, поскольку к последним

---

[1] См. подробнее: Макаров Д.И., Шевченко О.И. «Цифровые технологии в банковской сфере» / Международный научный журнал «Символ науки» # 12-1-1, Уфа, 2023

[2] См. об этом: Мещеряков, В. А. О понятии электронно-цифрового отображения в цифровой криминалистике / В. А. Мещеряков, О. Ю. Цурлуй // Российское правосудие. – 2022. – № S1. – С. 162-171. – DOI 10.37399/issn2072-909X.2022.SI.162-171. – EDN KNIWBY.

относятся помимо цифровых еще и иные нецифровые (аналоговые) методы передачи и обработки информации.

В связи с чем, можно определить, что цифровые технологии, как и аналоговые технологии, являются подвидом информационных технологий, которые в отличие от них основаны на двоичном коде.

Таким образом, цифровые технологии – это технологии, использующие совокупность средств и методов собирания, обработки, накопления и передачи криминалистически значимой информации сбора, обработки, накопления и передачи данных (первичной информации) для получения информации нового качества о состоянии объектов, процессов, явлений с использованием цифрового (двоичного) кода.

Рассматривая теоретическое определение информационных технологий важно следует выделить составные элементы, вкладываемые в понятие цифровых технологий.

Так, основными признаками информационных технологий являются:

- Направленность на обработку информации, что выражается в автоматизации рутинных операций, в частности, что информационные технологии позволяют автоматизировать процессы сбора, ввода, сортировки, классификации и хранения данных, которые ранее выполнялись вручную. Это существенно сокращает время и снижает вероятность ошибок. Помимо этого, они систематизируют и структурируют данные, то есть делают её легкодоступной, управляемой и пригодной для дальнейшего анализа. Помимо этого, информационные технологии позволяют не просто хранить, но и обрабатывать информацию, выявляя скрытые связи, закономерности;

- Использование технических средств (аппаратное обеспечение). Данный признак выражается в том, что технические средства опираются на физические устройства (аппаратное обеспечение или "железо"), которые выполняют функции обработки, хранения, передачи и вывода информации. Именно технические

средства (процессоры, оперативная память, жесткие диски, сетевые адаптеры) позволяют информационным технологиям обрабатывать объемы информации с высокой скоростью, что невозможно при ручном подходе. Они обеспечивают масштабируемость информационных систем.

Учитывая многообразие существующих и использующихся в повседневной деятельности человека информационных технологий, в целях дальнейшего анализа возможности их применения как в деятельности следователя по расследованию преступлений, так и в целом в ходе их использования в юриспруденции, следует классифицировать общие виды информационных технологий, которые используются человеком во всех сферах его деятельности.

Рассматривая виды информационных технологий, существующие в настоящее время и используемые в настоящее время в различных сферах деятельности, следует привести классификации данных технологий по различным основаниям.

Классифицируя информационные технологии по системам исчисления, лежащим в основе, выделяются следующие:

- компьютерные информационные технологии – информационные технологии, основанные на двоичной системе единиц и нулей[1];

- информационные технологии, не связанные с компьютерными, то есть не использующими двоичную систему[2]. К таким информационным технологиям можно отнести: книги, газеты, пишущие машинки, типографии. Кроме этого, в данную группу следует отнести и аналоговые средства связи: телеграф, телефон; средства аналоговой записи: магнитофоны, видеомагнитофоны, запись изображения на светочувствительную плёнку. К данной группе информационных

[1] См. об этом: Россинская Е. Р., Шамаев Г. П. Новый раздел криминалистики: криминалистическое исследование компьютерных средств и систем // Baikal Research Journal. 2015. Т. 6, № 1. С. 19.

[2] См.: Стяжкина, С.А. Информация как объект уголовно-правовой охраны: понятие, признаки, виды / С.А. Стяжкина // Вестник Удмуртского университета. - 2015. - С. 45-52.

технологий также относится микрофильмирование или микрофиширование: хранение большого объема текстовой и графической информации на плёнке в уменьшенном виде.

Обращаясь к классификации информационных технологий по типу решаемых задач, их можно разделить на следующие виды:

- Технологии обработки данных (Бухгалтерские системы, системы управления складами, системы обработки транзакций). Представляют собой Совокупность методов, инструментов и процедур, используемых для сбора, хранения, преобразования, анализа и вывода (представления) данных. Это фундаментальный уровень работы с информацией.

- Технологии управления (Информационные системы управления предприятием, системы поддержки принятия решений). От технологий обработки данных они отличаются тем, что направлены на поддержку принятия управленческих решений, оптимизацию операционной деятельности, повышение эффективности работы предприятия в целом.

- Офисные технологии (Автоматизация повседневной работы - текстовые редакторы, электронные таблицы, презентации, почтовые клиенты).

- Экспертные технологии (Экспертные системы, системы распознавания образов, машинное обучение, нейронные сети). Указанный вид информационных технологий характеризуется тем, что они стремятся имитировать или превосходить человеческие когнитивные способности (обучение, распознавание, принятие решений, прогнозирование, выявление закономерностей) на основе анализа больших объемов данных или знаний, полученных от экспертов. Принцип их работы заключается в том, что они используют сложные алгоритмы (например, нейронные сети) для решения поставленных задач. Основной их целью является ассистирование или замена человеческого интеллекта в конкретных областях, предоставляя рекомендации, прогнозы, классификации, диагнозы. Примером их использования уголовном судопроизводстве являются

программы для распознавания лиц/голосов, системы поддержки принятия решений для следователей.

Классифицируя информационные технологии по возможностям взаимодействия между собой следует выделить следующие виды:

- Локальные информационные технологии. Данный вид информационных технологий заключается в его функционировании на одном устройстве без сетевого взаимодействия. В качестве примера можно привести отдельный компьютер с установленным на нем программным обеспечением.

- Сетевые информационные технологии, суть которых заключается во взаимодействии устройств и пользователей через локальные или глобальные сети. Примерами могут служить корпоративные сети, Интернет, телефон, клиент-серверные системы, корпоративные сети. Отличительной их особенностью является обмен данными, совместная работа и удаленный доступ.

- Облачные информационные технологии. Также заключаются в обмене данных между пользователями. Вместе с тем отличительной особенностью указанных информационных технологий является обмен данных через облачные хранилища с использованием сети Интернет[1].

Классифицируя информационные технологии по сфере применения (применительно к процессу расследования преступлений) выделяются следующие[2]:

- Криминалистические информационные технологии (Специализированные технологии для сбора, анализа и представления цифровых доказательств. Программы для восстановления данных, анализа логов, исследования мобильных устройств).

---

[1] См. об этом: Рязанцева, М. П. Информационные технологии в криминалистике / М. П. Рязанцева // Научный электронный журнал Меридиан. – 2020. – № 1(35). – С. 216-218. – EDN CWJRWP.

[2] См. подробнее: Соколов, Ю. Н. Информационные технологии и оборот цифровых данных в криминалистике / Ю. Н. Соколов. – Екатеринбург : Федеральное государственное бюджетное образовательное учреждение высшего образования "Уральский государственный юридический университет", 2023. – 328 с. – ISBN 978-5-6049106-1-0. – EDN EGYKTJ.

- Информационные технологии в финансовой сфере. К данной группе относятся системы для обработки платежей, анализа транзакций, противодействия отмыванию денег.

- Геоинформационные технологии: Системы для работы с пространственными данными. Картографические сервисы, системы для визуализации мест происшествий.

Выделив основные виды информационных технологий, используемых повсеместно во всех сферах деятельности человека, необходимо более подробно остановиться на тех их видах, которые используются и могут быть использованы в юриспруденции, а также в сфере уголовного судопроизводства.

Для создания эффективных алгоритмов и криминалистических рекомендаций по комплексному практическому использованию современных информационных технологий в расследовании преступлений необходима их систематизация и детальный анализ. Следует выяснить, какие виды информационных технологий используются в юриспруденции, и в каких именно сферах и видах судопроизводства применяются, а том числе какие из информационных технологий применяются в уголовном судопроизводстве и в том числе в сфере досудебного производства по уголовным делам.

С этой целью мы сделаем попытку создания единой классификации информационных технологий, используемых в юридической практике а именно в уголовном судопроизводстве, в зависимости от различных оснований.

Мы считаем, что для всестороннего изучения информационных технологий в сфере уголовного судопроизводства, следует классифицировать их *по функциональному назначению, по типу используемых информационных технологий*, а также *в зависимости от стадии судопроизводства.* Ниже будут представлены сами классификации.

По функциональному назначению в уголовном судопроизводстве выделяются следующие:

- *Информационно-справочные системы.* Представляют собой базы данных и программные комплексы для хранения, систематизации и а также для предоставления юридически значимой информации, необходимой для расследования и рассмотрения уголовных дел. Примерами таких систем могут служить: Справочные Правовые Системы (СПС) типа "КонсультантПлюс" и "Гарант"; ГАС «Правосудие», ведомственные информационные системы МВД России; информационные системы Следственного комитета РФ. Они используются для учета уголовных дел, контроля за ходом расследования, формирования статистической отчетности, специализированные экспертно-криминалистические базы данных. Применяются в экспертных учреждениях (например, базы следов пальцев рук, ДНК, баллистические учеты) для проведения экспертиз и идентификации.

- *Документооборот и делопроизводство.* Данные системы обеспечивают обмен документами, регистрацию входящей и исходящей корреспонденции, размещение сведений о рассматриваемых делах, учет и хранение документов, необходимых в работе. Они используются следующим образом. В судах они предназначены для ведения судебных дел, включающее регистрацию исковых заявлений, контроль за их движением и исполнением; в адвокатских бюро и юридических фирмах используются для управления клиентскими досье, составления договоров на оказание услуг, подготовке исков, ходатайств и возражений; в нотариате предназначены для оформления проектов документов; в юридических отделах компаний они используются для разработки, согласования, подписания и хранения договоров с контрагентами, учредительных документов, протоколов собраний.

- *Сбор, фиксация и исследование доказательств.* Совокупность информационно-технических средств, направленных на выявление, фиксацию и изъятие материальных следов;

- *Коммуникация и дистанционное взаимодействие.* Среди них можно выделить системы видео-конференц-связи, используемые как в судах общей

юрисдикции, так и в арбитражных судах, а также с 2022 года и следователями в деятельности по расследованию преступлений. Кроме этого, к данной группе можно отнести электронный документооборот с подписанием документов электронно-цифровой подписью, а также получение справок, выписок, подача заявлений в государственные органы через портал "Госуслуги".

По типу используемых технологий, информационные технологии, используемые в юриспруденции, классифицируются следующим образом. Данная классификация является более технической.

К таким технологиям относятся:

- Базы данных и СУБД (системы управления базами данных). Данные технологии используются для хранения и управления всей процессуальной информацией, назначением которых является организация систематизированного хранения, эффективного доступа и надежного управления всей процессуальной информацией в юриспруденции.

- Сети и телекоммуникации. Используются в свою очередь для обеспечения связи (ВКС, электронный обмен данными), используемыми для обеспечения бесперебойной связи, включая видеоконференцсвязь и электронный обмен данными, в юридической сфере.

- Информационно-аналитические системы, которые используются для обработки больших объемов данных, машинного обучения, в том числе с использованием искусственного интеллекта.

- Средства кибербезопасности, применяемые для защиты информации, электронных подписей, шифрования;

- Периферийное оборудование, к которому относятся в числе прочего устройства для сбора биометрических данных, сканеры, принтеры.

В зависимости от стадии процесса информационные технологии подразделяются на следующие виды:

- информационные технологии, используемые в оперативно-розыскной деятельности и на стадии проверки сообщений о преступлениях (доследственной проверки).

- информационные технологии, используемые на стадии предварительного расследования.

- информационные технологии, используемые при рассмотрении уголовных дел в судах.

Полагаем, что информационные технологии, используемые на стадии предварительного следствия в следственной практике применительно к расследованию преступлений в сфере экономики в зависимости от их предназначения можно разделить на следующие группы:

1. Информационно-справочные и аналитические системы:

- Криминалистические информационные системы (базы данных). К числу таких можно отнести дактилоскопические и ДНК учеты МВД России, учеты оружия (пуль и гильз), иные криминалистические учеты. Помимо этого, сюда же можно отнести и базы данных различных ведомств (ЕГРЮЛ, ЕГРИП, ЕГРН, закрытые ИБД, ФИС-ГИБДД и иные):

- Правовые информационные системы, которые необходимы для применения действующего законодательства, поиска юридической практики (Гарант, Консультант и иные):

- Прогнозно-аналитические системы. Указанные информационные системы разработаны для проведения анализа больших объемов данных: их сведения из различных источников: показания свидетелей, данные с мест происшествий, цифровые следы, финансовые транзакции, базы данных, социальные сети и т.д. Данные системы способны обрабатывать и анализировать эти данные значительно быстрее и эффективнее, чем человек. Данные системы могут обнаруживать неочевидные корреляции, паттерны поведения, связи между лицами, местами и событиями, которые могут быть упущены при традиционном ручном анализе.

Кроме этого, существуют и программно-аналитические системы, направленные на поиск и идентификация объектов, в том числе лиц (в том числе находящихся в розыске). Одним из таких примеров может служить недавно введенная в действие система, находящаяся в пользовании МВД России (ГАИС «Сфера»), направленная на идентификацию и выявление в общественных местах лиц, находящихся в розыске по их портретному изображению.

К этой же категории информационных технологий относятся и программные комплексы для построения алгоритмов расследования преступлений.

2. Системы электронного документооборота и управления следственным процессом:

- Электронное уголовное дело (ЭУД). Вопросы создания и постепенного введения электронного уголовного дела на протяжении пяти лет является дискуссионным вопросом в разрезе эффективности его внедрения в Российское судопроизводство. В настоящее время в ряде зарубежных стран в целях эффективности документооборота вводится возможность его ведения в электронном формате.

- Системы межведомственного электронного взаимодействия, то есть возможность электронного взаимодействия между государственными органами, направление запросов между государственными органами и истребование необходимой для расследования информации;

- Автоматизированные рабочие места (АРМ) следователя/дознавателя, что представляет собой информационно-телекоммуникационную систему, предусматривающую возможность загрузки туда документов, их подписание и отправку. Помимо этого, такие системы предоставляют доступ к базам данных, справочникам, законодательству, а также обеспечивает отслеживание сроков исполнения задач, а также входящих документов[1].

[1] См. об этом: Вехов В. Б. Понятие и возможности автоматизированных рабочих мест сотрудников правоохранительных органов как технико-криминалистических средств // Вестник Волгоградской академии МВД России. 2010. №1 (12); Колычева А.Н. Автоматизированное

3. *Информационные технологии, предназначенные для поиска и фиксации криминалистически значимой информации.*

К данной группе относятся:

- Цифровая криминалистика (Digital Forensics). Является процессом идентификации, сохранения, анализа и представления данных, извлеченных с цифровых устройств, с целью расследования преступлений. Так, указанное направление криминалистики включает в себя систему методик, направленных на получение информации с компьютеров, мобильных телефонов, серверов, облачных хранилищ и других цифровых носителей, в том числе и с серверов операторов связи и организаций, обеспечивающих передачу электронных сообщений по сетям связи, а также их исследование, в целях поиска доказательственной информации, направленной на установление юридически важных для расследования связей, событий, выяснение круга лиц.

- Средства фиксации следственных действий. К указанной группе можно отнести такие информационные технологии как видеокамеру, кинокамеру, диктофон, фотоаппарат и некоторые другие;

- Экспертные системы и специализированное программное обеспечение, предназначенное для криминалистических экспертиз, которые необходимы для проведения исследований электронных носителей информации и иных предметов, на которых могут иметься следы преступления.

4. Информационные технологии, используемые для коммуникации и дистанционного взаимодействия:

- Видео-конференц-связь (ВКС), которая может использоваться для проведения следственных действий, таких как допрос, очная ставка и предъявление для опознания. Видео-конференц-связь используется как средство для проведения следственных действий в дистанционном формате, чаще всего в

рабочее место следователя: современные возможности и организация труда // Научный вестник ОрЮИ МВД России им. В. В. Лукьянова. 2023. №3 (96).

случаях, при которых участники судопроизводства проживают на значительном удалении от места производства следственного действия[1].

Указанная технология обеспечивает возможность дистанционного проведения допросов, очных ставок, предъявлений для опознания, что решает проблему обеспечения явки лиц, проживающих на большом расстоянии от места производства следственного действия, что положительным образом влияет на сроки предварительного следствия.

- Системы электронных уведомлений. Используются для оперативного оповещения участников процесса о проведении следственных и иных процессуальных действий. Законодательно оповещение участников процесса посредством СМС закреплено на судебных стадиях, вместе с этим, такое оповещение используются и следственными органами на стадии расследования. Посредством СМС участникам процесса направляются уведомления и повестки о необходимости явки для производства следственных и процессуальных действий.

Описанные выше информационные технологии, используемые на стадии предварительного следствия при расследовании преступлений в сфере экономики, представлены в Приложении №1 к исследованию в виде схемы.

Тем не менее, криминалистические рекомендации разрабатываются не только для следователей, но и для суда. Криминалистическим особенностям использования информационных технологий на этапе судебного разбирательства по уголовным делам в юридической науке уделялось должное внимание учеными криминалистами.

Так, Ю.В. Кореневским описаны особенности судебного следствия, особенностям поддержания государственного обвинения[2]. И.В. Румянцевой проанализированы проблемы поддержания государственного обвинения в суде 1

---

[1] См. об этом: Плетникова М.С., Семёнов Е.А. К вопросу использования видеоконференцсвязи при производстве допроса // Вестник Уральского юридического института МВД России. 2021. №1.

[2] См. об этом Кореневский, Ю.В. Криминалистика для судебного следствия /Ю.В. Кореневский. -М.: АО «Центр Юринфор», 2001. 198 е

инстанции[1]. В свою очередь А.А. Корчагиным на монографическом уровне описаны особенности судебного следствия по уголовным делам об убийствах[2].

Вопросам влияния информационных технологий на судопроизводство на этапе судебного следствия посвящены работы Н.Г. Муратовой, О.В. Федоровской, Н.Н. Шаталова и других.

В результате анализа научной литературы и изучения юридической практики нами выделены основные направления информационных технологий в судебной практике, которые как используются в настоящее время в практике деятельности судов и нуждаются только в усовершенствовании их использования, а также те направления, которые еще не используются, но их использование существенно облегчило бы деятельность судов, в том числе посредством автоматизации рутинных операций, выполняемых сотрудниками судов ежедневно и фактически занимающих большое количество рабочего времени.

К таким направлениям мы относим следующие:

- Системы электронного документооборота в судах: Подача заявлений, ходатайств, обжалований в электронном виде.
- Видео-конференц-связь в судебных заседаниях: Проведение дистанционных допросов свидетелей, потерпевших, участия в заседаниях заключенных. Проблемы с идентификацией и обеспечением безопасности.
- Базы данных судебных решений: Доступ к судебной практике для участников процесса.
- Использование мобильных устройств для синхронного перевода показаний лиц (электронные переводчики).

---

[1] См. подробнее Румянцева И.В. Ситуационный подход в судебном следствии суда I инстанции: Дис. ... канд. юрид. наук. - Калининград, 2004. - С. 112.

[2] См. подробнее Корчагин, А. А. Криминалистическое обеспечение предварительного и судебного следствия умышленных убийств: теория и практика / А. А. Корчагин. – Москва: Издательство "Юрлитинформ", 2021. – 424 с. – (Библиотека криминалиста). – ISBN 978-5-4396-2241-2. – EDN IGTSVR.

- Использование автоматических преобразователей аудиофайлов (записанных на диктофон)

- Вопросы разработки электронного преобразователя аудиофайлов для аудио протоколирования в судебном заседании.

- Информационно-аналитические системы для обработки оперативных данных. Данные системы служат для сбора, систематизации и анализа оперативных данных в реальном времени. Они позволяют выявлять связи между лицами, объектами и событиями и обнаруживать закономерности в преступной деятельности. Данные системы направлены на ускорение поиска и анализа информации и объектов.

- Системы распознавания лиц, номеров. Они позволяют быстро находить разыскиваемых лиц или транспортные средства путем сравнения изображений с базами данных. Эти системы помогают устанавливать маршруты передвижения подозреваемых или свидетелей, анализируя видеопотоки с камер наблюдения.

- Мониторинг информационного пространства – это целенаправленный сбор и анализ данных из открытых онлайн-источников для выявления угроз и преступной активности. Он позволяет обнаруживать информацию о готовящихся преступлениях или лицах, представляющих оперативный интерес, до того, как они произойдут. Системы мониторинга идентифицируют связи между пользователями, анализируют их настроения и намерения[1].

[1] См. об этом: Волгин Ю.В., Черненко Т.Г. Использование многомерной модели представления оперативно-розыскной информации при разработке информационных систем, используемых в процессе раскрытия преступления // Юридическая наука. 2020. №1; Дивольд В. Е. Информационно-аналитическая система оперативно-розыскной информации как важнейшая составляющая оперативно-аналитического обеспечения розыскной деятельности // Вестник БелЮИ МВД России. 2022. №4; Саркисян Г.Г. Теоретическая и правовая основы оперативно-аналитической деятельности органов внутренних дел Российской Федерации: основные выводы и предложения // Труды Академии управления МВД России. 2023. №4 (68).

1.2. Криминалистические особенности преступлений в сфере экономики, обусловливающие необходимость применения информационных технологий при их расследовании

На современном этапе преступления, совершенные в сфере экономики отличаются высоким уровнем организованности и профессионализма исполнителей, характеризуются активным использованием современных информационных технологий и инструментов сокрытия следов преступной деятельности. Нередко такие деяния сопровождаются созданием фиктивных юридических лиц, подделкой документов и манипуляциями с бухгалтерской отчетностью для ухода от налогов и легализации незаконно полученных доходов. Данные преступления часто выходят за пределы одной страны и требуют международного сотрудничества правоохранительных органов для их расследования.

Анализируя направления использования современных информационных технологий в следственной практике, а также особенности их использования при расследовании преступлений в сфере экономики необходимо выяснить, какие преступления к ним относятся и установить суть иных, на первый взгляд, синонимичных понятий, таких как «экономические преступления», «преступления в сфере экономической деятельности», «преступления экономической направленности», вместе с тем, которые имеют разное содержание, а также являются разными «по объёму».

Из всех вышеперечисленных определений наиболее широким понятием является «преступления в сфере экономики». Так, если обратиться к разделу VIII Уголовного Кодекса РФ, указанный раздел включает в себя большой пласт преступлений, среди которых как преступления против собственности, преступления в сфере экономической деятельности, так и преступления против службы в коммерческих организациях. Таким образом, данное определение является наиболее объёмным из вышеперечисленных.

При этом, например, преступления в сфере экономической деятельности, включенные в Главу 22 УК РФ, входят в раздел VIII этого же нормативного акта, что означает, что определение «преступления в сфере экономической деятельности» являются частью от целого, где целым являются "преступления в сфере экономики.

Анализируя определение «преступления экономической направленности», следует обратиться к нормативному его закреплению, которое содержится в указании Генпрокуратуры России N 462/11, МВД России N 2 от 25.06.2024 "О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности". В данном документе содержится перечень преступлений, которые при заполнении документов статистической отчетности следует указывать как преступления экономической направленности. Какого-либо диспозитивного определения данный документ не содержит. Вместе с тем, анализируя его содержание, можно прийти к выводу, что под преступлениями экономической направленности подразумеваются преступления, включенные как в раздел преступлений против собственности, преступлений в сфере экономической деятельности, так и преступлений против службы в коммерческих организациях, объективная сторона совершения которых затрагивает правоотношения, связанные с финансово-хозяйственной деятельностью организаций.

«Экономические преступления» – это обиходное понятие, которое нормативно нигде не закреплено. В источниках это определение трактуется различно, но значение сводится к тому, что «экономические преступления» – это противоправные деяния, посягающие на установленный порядок экономических отношений, причиняющие ущерб[1].

[1] См. об этом: Мажитова С.Р. О проблеме определения понятия «Экономическая преступность» (экономические преступления // Вестник ЧелГУ. 2011. №35; Тактоева В. В. Понятие экономической преступности и проблемы квалификации преступлений в сфере экономики // Криминалистика: вчера, сегодня, завтра. 2018. №2 (6); Вытовтов А.Е. Еще раз к понятию экономических преступлений в российском уголовном законодательстве // Пробелы в российском законодательстве. 2023. №4.

Поскольку наиболее объёмным определением из вышеперечисленных является определение «преступления в сфере экономики», то дальнейший анализ направлений применения современных информационных технологий будет проводиться применительно к данным преступлениям.

В нашем исследовании проблемы применения информационных технологий рассмотрены в контексте их применения при расследовании преступлений в сфере экономики, то есть наиболее объемной группой преступлений, которая включает как преступления в сфере экономической деятельности, так и иные преступления против собственности, совершенные в процессе финансово-хозяйственной деятельности организаций, а также против интересов службы в коммерческих и иных организациях. Данные престуления с точки зрения криминалистики обладают схожей следовой картиной и рядом общих признаков.

С.Ю. Журавлевым представлена авторская классификация разновидностей преступной деятельности при анализе преступлений в сфере экономики[1]. К ним относятся: преступления, связанные с причинением имущественного ущерба собственнику или иному владельцу имущества; хищением чужого имущества или приобретение на него права, в том числе и путем обмана или злоупотребления доверием; присвоение или растрата чужого имущества; осуществление запрещенной законом деятельности; уклонение от уплаты налогов и платежей; ограничение конкуренции; нарушение регистрационных и реорганизационных процедур в сфере экономической деятельности; приобретение и сбыт имущества, заведомо добытого преступным путем; легализация денежных средств или иного имущества, приобретенных другими

[1] См. подробнее: Журавлев С.Ю. Методологические основы совершенствования методики расследования преступлений в сфере экономики : автореферат дис. ... доктора юридических наук : 5.1.4. / Журавлев Сергей Юрьевич; [Место защиты: ФГКОУ ВО «Нижегородская академия Министерства внутренних дел Российской Федерации»]. - Нижний Новгород, 2022. - 59 с.

лицами преступным путем; злоупотребления служебными (должностными) полномочиями и ряд иных преступлений, способствующих преступной деятельности в сфере экономики.

Такой объемный выбор вида анализируемых преступлений сделан неспроста, ведь данные преступления обладают определенными особенностями, отличающими их от иных преступлений, и регламентированных в других главах Уголовного закона, но и в то же время обладающими рядом общих признаков, анализ которых нами представлен в данном параграфе далее.

Перед началом более глубокого анализа признаков и отличительных особенностей преступлений в сфере экономики, следует выделить несколько основных характеристик.

Во-первых, это причинение ущерба от преступлений. При этом, ущерб от данных преступлений может быть причинен как отдельным лицам и организациям – по преступлениям связанным с хищением имущества, незаконным использованием товарного знака и некоторым другим, так и государству - по преступлениям, связанным с хищением государственной собственности и по иным преступлениям, в том числе в сфере неуплаты обязательных платежей, ограничения конкуренции, осуществления незаконной предпринимательской деятельности и ряду других преступлений, которые, несмотря на отсутствие прямого материального ущерба от совершенных действий, подрывают экономическую стабильность государства, а также посягают на основы порядка ведения экономической деятельности, регулятором которого является государство.

Во- вторых, указанные преступления обладают высокой латентностью, что связано с интеллектуальным характером их совершения, сокрытия и маскировки.

Сложность и специфика данных преступлений, а также активное применение в данной сфере современных информационных технологий

обуславливают актуальность изучения криминалистических особенностей данных преступлений для их эффективного раскрытия и расследования.

Выделяя особенности способа совершения преступления, совершенного в сфере экономики важно выделить, что данные преступления имеют интеллектуальный ненасильственный характер. При совершении преступлений злоумышленниками используются такие способы как: обман, злоупотребление доверием, имитация законных операций, фальсификация документов, использование сложных финансовых схем, использование для совершения преступления должностного положения, специальных знаний[1].

Более того, данные преступления требуют длительного и детального планирования. Их отличает высокая степень подготовки, выражающаяся в маскировке под легальную деятельность, подделке документов и использовании изощренных финансовых инструментов.

Данные действия являются многостадийными, поскольку развиваются в несколько этапов: предварительная подготовка, непосредственное совершение и последующее сокрытие следов[2].

Кроме этого, в совершении и сокрытии этих преступлений широко применяются информационные технологии – компьютерные системы, интернет и электронные платежи.

Помимо этого, такие преступлений часто совершаются в составе группы лиц по предварительному сговору, организованными группами, где имеет место явное разграничение особенностей и ролей.

---

[1] См. например: Манукян А.Р. Экономические преступления в условиях цифровизации // Проблемы экономики и юридической практики. 2020. №1.

[2] См.: Журавлев, С.Ю. Знание о механизме экономических преступлений и его применение в процессе построения методик расследования / С.Ю. Журавлев. - Текст : непосредственный // Вестник научных школ Нижегородской академии МВД России : сборник статей / под науч. ред. М.П. Полякова. - Нижний Новгород : Нижегородская академия МВД России, 2011. - С. 251-264.

При описании криминалистических особенностей преступлений в сфере экономики важно также рассмотреть особенности субъектного состава таких преступлений, особенности предмета преступного посягательства, а также особенности следовой картины таких преступлений и проблемы выявления и доказывания объективной стороны таких преступлений.

Рассматривая особенности субъектного состава рассматриваемого вида преступлений, следует отметить, что субъекты совершения данных преступлений обладают в большинстве своем высшим образованием, занимают руководящие должности или имеют специальные познания в экономической сфере. Нередко такие преступления совершаются с использованием служебного положения, доступа к ресурсам, информации, документам. Яркими примерами могут служить: мошенничество с использованием служебного положения, присвоение или растрата, злоупотребление служебными полномочиями руководителем коммерческой организации[1].

Преступления рассматриваемого вида совершаются в большинстве своем после подробного их планирования, продумывания путей отхода и способов сокрытия следов, в числе которых уничтожение значимых для расследования уголовного дела документов, фальсификация отчетности, а также в дальнейшем и оказание давления на свидетелей, использование коррупционных связей.

Наиболее распространенным предметом преступного посягательства по преступлениям рассматриваемого вида являются денежные средства, ценные бумаги, имущественные права, иное имущество, имеющее цифровую или документарную форму выражения[2]. Обстановка совершения таких преступлений

---

[1] См. об этом: Варданян А.В., Казаков В.В. Криминалистический анализ субъектов преступлений, связанных с воспрепятствованием законной предпринимательской или иной деятельности, как фактор повышения результативности расследования // Всероссийский криминологический журнал. 2015. №4.

[2] См. подробней: Коняхин В.П., Асланян Р.Г. Информация как предмет и средство совершения преступлений в сфере экономической деятельности // Российский следователь. 2016. N 8. С. 24 - 27

часто не имеет четко выраженного места совершения преступления. Основные действия, направленные на совершение таких преступлений происходят как в административных зданиях, в офисах, кредитных учреждениях, равно как и могут совершаться удалено и дистанционно с доступом в сеть Интернет, в том числе с использованием интернет-банкинга для совершения платежей. Кроме этого, преступные действия часто маскируются под законные операции, проводимые в рамках гражданско-правовых отношений или регулируемые специальными нормативными актами.

Изучая следовую картину таких преступлений важно отметить сочетание идеальных и материальных следов, в том числе «электронных». Материальные следы в большинстве своем содержатся в документах, в числе которых: финансовые документы (договоры, счета, платежные поручения, бухгалтерская отчетность), бумажная переписка. «Электронные» следы, рассматриваемые нами как подвид материальных следов – это данные о доступе к информационным системам, электронные документы, в том числе и сведения из Интернет-банкинга платежные поручения, сформированные с их помощью сведения о движении денежных средств по счетам, электронная переписка, метаданные файлов. При этом, с учетом активно используемого субъектами хозяйственной деятельности электронного документооборота, электронных средств коммуникации и оплаты, отмечается преобладание «электронных следов» среди материальных.

К идеальным следам относятся показания потерпевших, свидетелей, соучастников преступлений[1].

Особенностями следовой картины преступлений в сфере экономики является рассредоточенность следов. Это означает, что документы и информация могут находиться в разных местах, в разных организациях и даже в разных

[1] См: Карепанов Н.В. Особенности образования и сущность следов преступлений в сфере экономической деятельности // Российское право: образование, практика, наука. 2024. №1

странах. Отмечается также отсутствие или минимальное количество традиционных материальных следов (следов рук, обуви и т.д.).

Также особенностями следовой картины данных преступлений являются трудности в их обнаружении и фиксации (при изъятии и закреплении следов требуется привлечение специалистов, обладающих специальными познаниями в различных отраслях экономики и информационных технологий).

Основными проблемами, с которыми сталкиваются следователи, расследующие данные преступления, являются их высокая латентность, выражающаяся в том, что преступления выявляются спустя длительный период времени с момента их совершения. Также они характеризуются большим объемом информации, переплетением законных и незаконных операций, необходимостью привлечения к расследованию специалистов как на этапе их выявления, изъятия, так и закрепления следов преступления, противодействием со стороны преступников, а также международным характером ряда преступлений (например, связанных с уклонением от таможенных платежей, выводом денежных средств за рубеж и рядом иных), что с учетом трудностей международного уголовного судопроизводства усложняет сбор доказательств.

Таким образом, для грамотной организации расследования преступлений данного вида, в том числе и с применением современных информационных технологий, важен комплексный и междисциплинарный подход к их расследованию, а также специализированная подготовка сотрудников правоохранительных органов в части использования современных информационных технологий и методов криминалистики для борьбы с данным видом преступности.

Преступления в сфере экономики, которые включают в себя преступления в сфере экономической деятельности, ряд преступлений против собственности, так и ряд преступлений против интересов службы в коммерческих организациях,

как сказано выше, обладают особенностями, отличающими их от других видов преступлений, закрепленных в уголовном законе. Предложения и рекомендации по применению современных информационных технологий, сформированные нами в тексте исследования, представлены применительно к процессу расследования преступлений в сфере экономики с учетом их отличительных признаков отличающих их от преступлений других видов.

Как говорилось ранее, в условиях глобальной цифровизации преступления в сфере экономики совершаются в большинстве своем с использованием современных информационных технологий. Таким образом, для фиксации следов, оставленных с применением информационных технологий, требуется, соответственно, их использование при расследовании преступлений исследуемого вида. Этим и обусловлено выделение нами данного вида преступлений в контексте использования современных информационных технологий в расследовании.

1.3 Основные направления применения информационных технологий в следственной практике при расследовании преступлений в сфере экономики

Рассматривая основные направления использования информационных технологий в деятельности следователя по расследованию преступлений, в сфере экономики, следует их структурировать и классифицировать по группам в зависимости от их фактического предназначения.

Изучая научную литературу и анализируя результаты практической деятельности следователей по расследованию преступлений, мы выделяем следующие группы направлений использования информационных технологий в следственной практике[1].

Группами направлений использования информационных технологий в следственной практике являются:

1. *Использование информационно-справочных и аналитических систем для поиска информации.* В данную группу направлений входит применение специализированных баз данных, доступ к криминалистическим учетам (дактилоскопическим, ДНК, баллистическим), розыскным базам, ведомственным информационным системам.

2. *Использование информационных технологий, предназначенных для фиксации следовой картины преступлений (средств сбора, фиксации и исследования доказательств).*

В указанную группу входят следующие направления использования информационных технологий[2]:

---

[1] См. подробней: Фролов В.В. Использование информационных технологий в расследовании: направления, проблемы и перспективы // Полицейская и следственная деятельность. 2023. №2.

[2] См. об этом: Варакин Я.Г. Криминалистические особенности фиксации, изъятия цифровых следов преступления и иной доказательственной информации, // Вестник СурГУ. 2021. №4 (34).

- Компьютерная и мобильная криминалистика: использование специализированного ПО и оборудования для извлечения, анализа данных с различных носителей (ПК, смартфоны, планшеты, "умные" устройства);

- Анализ облачных данных: практика получения данных от провайдеров (в том числе через международное сотрудничество), проблемы с юрисдикцией и шифрованием;

- Работа с большими данными: применение аналитических систем (например, аналитика финансового мониторинга) для выявления подозрительных транзакций, связей, аномалий в поведении.

- Активное применение открытых источников для сбора досье, выявления контактов, построения хронологии событий. Использование Интернета при расследовании преступлений.

- Видео - и аудиофиксация: применение для фиксации следственных действий (осмотры, обыски, допросы, следственные эксперименты) как гарантия законности и доказательственной базы.

*3. Использование информационных технологий для коммуникации и дистанционного взаимодействия***.** В данную группу включаются несколько актуальных в настоящее время направлений использования информационных технологий.

В их числе:

- Видеоконференцсвязь, а также связанные с ее использованием аспекты применения электронно-цифровой подписи, направленные на возможность удаленного подписания процессуальных документов. Например, возможность выхода лицом на связь с судом посредством своего ПК и возможность заверения данных им показаний посредством электронно-цифровой подписи[1];

- Вопросы оформления ЭЦП участникам процесса.

---

[1] См. подробней: Плахота К.С. Использование видео-конференц-связи при расследовании преступлений // Вестник КРУ МВД России. 2021. №3 (53); Фарафонова О.А. Использование видео-конференц-связи в уголовно-процессуальном производстве // Научный вестник ОрЮИ МВД России им. В. В. Лукьянова. 2024. №4 (101).

4. Использование информационных технологий для организации предварительного следствия.

К числу указанных направлений следует отнести:

- Проблемы применения синхронных переводчиков в процессе расследования;

- Вопросы ведения уголовного дела в электронном виде;

- Использование ГИС-технологий - нанесение на карты мест происшествий, маршрутов передвижения, географического распределения преступлений.

- Использование программных комплексов для построения алгоритмов расследования преступлений:

- Использование информационных технологий в целеопределении и планировании следственных действий.

5. Использование информационных технологий для электронного документооборота и управления следственным процессом. Данная группа направлений включает в себя электронный документооборот и автоматизацию процессов: использование информационных систем для регистрации сообщений о преступлениях, учета уголовных дел, формирования отчетов[1].

Для наглядности направления использования информационных технологии в деятельности по расследованию преступлений представлены схематично в Приложении № 2 к исследованию.

Проблемы применения информационных технологий, предназначенных для фиксации следовой картины преступлений, в которую входят и проблемы изъятия электронных носителей информации при расследовании преступлений, проблемы получения электронной информации о переписках у операторов и провайдеров, проведения допросов с использованием видеоконференцсвязи подробно раскрыты во второй главе исследования.

---

[1] См.: Бычков В. В., Вепрев С. Б. Электронный документооборот в следственной деятельности: проблемы и пути их решения // Правопорядок: история, теория, практика. 2018. №4 (19).

При этом отдельные проблемы применения информационных технологий, не предназначенных для фиксации следовой картины преступлений, также требуют внимания.

Так, немало важным вспомогательным элементом, используемым в качестве ориентирующего вектора при планировании следственных действий при расследовании преступлений в сфере экономики, является использование информации, содержащейся в информационных базах данных. Среди них – как базы, находящиеся в открытом доступе (ЕГРЮЛ, ЕГРИП, Публичная кадастровая карта и иные), так и сведения, содержащиеся в ведомственных учетах.

Использование баз данных правоохранительными органами играет все более значительную роль в расследовании преступлений в сфере экономики. Сложность и многогранность этих преступлений, часто включающих в себя сложные финансовые схемы, трансграничные операции и использование современных технологий, делают эффективный поиск и анализ информации критически важным. Базы данных, содержащие информацию о финансовых транзакциях, регистрационных данных компаний, движении имущества и коммуникациях, становятся незаменимым инструментом для раскрытия преступлений в этой сфере.

Как утверждает П.С. Пастухов, выявление и расследование преступлений в сфере экономики наиболее эффективно осуществляется с помощью современных информационных технологий и баз данных, отслеживающих движение товаров, финансов и иных юридически значимых действий[1].

Так, к примеру, большое количество необходимой ориентирующей информации можно получить при использовании баз данных Федеральной

[1] См.: Пастухов П.С. Базы данных как источники доказательственной информации в расследовании преступлений в сфере экономической деятельности // Пермский юридический альманах. Пермь, 2020

налоговой службы – Единый государственный реестр юридических лиц (ЕГРЮЛ) и Единый государственный реестр индивидуальных предпринимателей (ЕГРИП). В базе данных ЕГРЮЛ содержится такой пласт информации как наименование организации, ее ИНН, ОГРН, адрес регистрации, сведения об адресе регистрации организации, ее учредителях и руководителях, сведения о видах экономической деятельности организации, о размере уставного капитала, сведения о держателе реестра акционеров (применительно к акционерным обществам), а также иная значимая информация. Таким образом, ЕГРЮЛ содержит сведения обо всех записях государственной регистрации при создании, реорганизации и ликвидации юридического лица. В ЕГРИП содержится информация аналогичного характера применительно к индивидуальным предпринимателям.

При расследовании преступлений в сфере экономики, где предметом преступного посягательства являлись земельные участки, либо преступлений, расследованием которых требуется установить характеристики земельных участков, зданий, иных объектов строительства, важно отметить в качестве вспомогательного средства такую базу данных как публичная кадастровая карта, запущенную Росреестром. Фактически указанная база данных предоставляет общедоступные сведения Единого государственного реестра недвижимости (ЕГРН).

Сервис «Публичная кадастровая карта» предоставляет общедоступную справочную информацию о недвижимости, включая кадастровую стоимость, номера, собственность, назначение и площадь объектов. На карте отображаются государственные и административные границы, зоны с особыми условиями использования территорий, а также контуры земельных участков, зданий и

сооружений[1]. База данных содержит сведения о более чем 60 миллионов земельных участков и 44 миллионов зданий и сооружений. Сервис пользуется высокой популярностью (более 8 миллионов пользователей в 2019 году), и информация в нём ежедневно обновляется.

Освещая тематику использования специальных ведомственных баз данных при расследовании преступлений необходимо обратить внимание на следующие. При этом, необходимо отметить, что сведения, содержащиеся в перечисляемых нами далее информационных базах носит конфиденциальный характер и предоставляется не иначе как на основании официального следственного запроса[2].

При расследовании преступлений, связанных с перевозкой грузов, поставкой каких-либо товаров, осуществляемых посредством автотранспорта, необходимо прибегнуть к ведомственным системам МВД России, например, ФИС-ГИБДД (содержит сведения о регистрации, собственниках автомобиля), также возможно обратиться к сведениям системы «Платон», содержащей сведения о местах передвижения транспортных средств с разрешённой максимальной массой свыше 12 тонн.

Так, при расследовании отдельных преступлений в сфере экономики, например, связанных с незаконным оборотом спиртосодержащей продукции, большой объём информации возможно получить в системе ЕГАИС. Данная система содержит информацию о каждой единице алкогольной продукции, включая регистрационный номер, данные о начале оборота, сведения об организации-уведомителе и производителе, наименование продукции (на разных

[1] Публичная кадастровая карта (ПКК), функционирующая на Единой цифровой платформе «Национальная система пространственных данных» (НСПД).URL: https://nspd.gov.ru/map?thematic=PKK&zoom=3.8824604466622987&coordinate_x=7393186.908732477&coordinate_y=7633543.829873955&baseLayerId=235&theme_id=1&is_copy_url=true (дата обращения – 30.09.2025)

[2] См. об этом: С. А. Черняков, С. Л. Горбатенко Актуальность использования ведомственных информационных онлайн-сервисов и автоматизированных баз данных МВД России в оперативно-розыскной деятельности // ППД. 2024. №1.

языках), крепость, объем тары, состав, срок годности, и реквизиты подтверждающих документов, а также данные о товарном знаке.

Следует перечислить и иные базы данных, в которых содержится информация, позволяющая эффективно проводить расследование различных преступлений в сфере экономики.

Например, базы данных Росреестра содержат информацию о недвижимости, земельных участках, их владельцах и сделках с ними. Такие базы данных могут быть использованы при расследовании мошенничеств с недвижимостью и других преступлений в сфере экономики, связанных с имуществом.

Базы данных банков и платежных систем содержат информацию о финансовых транзакциях, о движении денежных средств. Указанная информация необходима при расследовании большого объёма преступлений в сфере экономики: мошенничеств, незаконной банковской деятельности и иных.

При расследовании преступлений, связанных с внешнеэкономической деятельностью, в частности, предусмотренных ст. 193, 193.1 УК РФ, а также преступлений, связанных с контрабандой, могут быть полезны базы данных таможенных органов, которые содержат информацию о товарах, пересекающих границу, их стоимости и владельцах.

Также следует не забывать и базы данных МВД, содержащие общие сведения о гражданах, лицах, их адресах – которые необходимы следователю для своевременного установления местонахождения интересуемых лиц и производства с ними необходимых следственных действий – ИБД, ОСК, «Розыск-Магистраль» и иные.

Использование баз данных кардинально меняет подход к расследованию преступлений, обеспечивая беспрецедентные возможности для сбора, анализа и обработки информации. Своевременное использование необходимых баз данных позволяют значительно ускорить расследование, повысить его эффективность. Зачастую именно получение информации, содержащейся в базах данных, играет

большое вспомогательное воздействие на планирование дальнейшее планирование следственных действий, тактику их производства, а также на установление лица, совершившего преступления. Сведения, полученные из таких источников, могут полагаться в основу доказательственной базы при расследовании преступлений. Таким образом, грамотное использование сведений, содержащихся в информационных базах, может внести существенный в вклад в расследование преступлений в сфере экономики, в том числе в той части, в которой это описано в настоящем параграфе.

Еще одним довольно обсуждаемым вопросом в контексте внедрения информационных технологий в уголовное судопроизводство, является создание электронных уголовных дел. Электронные уголовные дела упростят решение многих процессуальных вопросов, таких как восстановление утраченных материалов, ознакомление участников процесса с материалами дела (в соответствии со статьями 158.1, 216, 217, ч. 2 и 3 ст. 225, ч. 4 ст. 226.7 УПК РФ), передача дел в апелляционные инстанции и возврат дел в суд первой инстанции (ст. 390 УПК РФ).

Е.А. Комарова и Г.А. Гундерич[1], высказывают мысль о том, что при рассмотрения практики ведения уголовных дел в электронном виде, отличительным примером может служить уголовное производство Республики Казахстан, которая позволяет вести уголовное судопроизводство как в бумажном, так и в электронном виде по усмотрению лица, ведущего процесс (с мотивированным постановлением о выборе формата и возможностью перехода на бумажный вариант при необходимости — ст. 42.1 УПК РК).

В теории уголовного процесса уже неоднократно высказывались предложения о переводе материалов уголовных дел в электронный формат, о целесообразности фиксации результатов следственных и иных процессуальных действий при помощи электронных средств. Авторы подчеркивают, что электронная форма может помочь уберечь материалы уголовного дела от

[1] См. об этом: Комарова Е.А., Гундерич Г.А. Внедрение информационных технологий в уголовное судопроизводство. / Право и государство: теория и практика, 2020.

умышленного уничтожения или повреждения[1]. Поэтому переход на электронную форму приведет к сокращению документооборота и обеспечит сохранность не только отдельных материалов, но и целых уголовных дел. Кроме того, это может улучшить качество расследования, поскольку облегчен доступ участников уголовного судопроизводства к материалам уголовного дела, а также упрощена процедура ведомственного контроля и прокурорского надзора.

По нашему мнению, переход уголовного судопроизводства в России на электронный формат вполне обоснованное предложение, к которому постепенно должно прийти как российское законодательство, так и практика. В настоящее время, отдельные элементы электронного делопроизводства уже начинают реализовываться в уголовном судопроизводстве РФ, в частности такими примерами может послужить постепенный переход государственных органов и ряда кредитных учреждений на получение и обработку запросов государственных органов исключительно в электронном виде без бумажного носителя.

Вместе с тем в настоящее время при обсуждении вопросов о внедрении электронного уголовного дела в отечественное уголовное судопроизводство необходимо проработать ряд ключевых вопросов, среди которых техническая оснащенность судов и следственных подразделений для ведения электронных уголовных дел, соответствующее программное обеспечение, функционирование взаимодействия на программном уровне между следственными подразделениями, оперативными подразделениями, органами прокуратуры и судом, возможность интеграции печатных документов в электронное уголовное дело, а также проработать вопросы обеспечения всех участников уголовного судопроизводства электронно-цифровыми подписями. В данной связи также необходимо уделить внимание проработке возможности участия в электронном уголовном деле лиц,

[1] См. подробней: Моругина Н. А. Электронное уголовное дело: понятие, история, зарубежный опыт, перспективы // Правопорядок: история, теория, практика. 2025. №1 (44); Шереметьев И. И. Электронное уголовное дело: что это такое и пути его создания // Lex Russica. 2020. №10 (167).

не использующих и не имеющих возможности приобрести технические средства (персональные компьютеры, смартфоны). В частности, для обеспечения категории лиц, не имеющих технические средства для получения определенных процессуальных документов, а также всего электронного уголовного дела в целом на стадии ознакомления с ним, предлагается использовать «электронные стойки-киоски» с возможностью доступа посредством сети Интернет к электронному виду уголовного дела.

Несомненно, проработка указанных вопросов и внедрение в уголовное судопроизводства электронного уголовного дела существенно сократит как финансовые вопросы, связанные с «ценой преступности», решит вопросы архивации уголовных дел, но и что немало важно повысит объективность расследования, связанную с постепенным уходом от протокольной формы и переходом на исключительно аудио-визуальную форму фиксации хода и результатов следственных и иных процессуальных действий.

Вместе с тем, многие вопросы, связанные с внедрением электронного судопроизводства в сферу уголовного, гражданского судопроизводства, которые еще предстоит детально разработать и постепенно внедрить в указанные сферы, в настоящее время успешно реализованы в сфере арбитражного судопроизводства.

В настоящее время электронное судопроизводство в судебной системе РФ в отличие от иных систем наиболее развито в арбитражных судах. Ярким примером опережения внедрения информационных технологий именно в арбитражное судопроизводство, в отличие от иных видов судопроизводств в РФ является возможность подачи заявления в арбитражные суды в электронной форме (ст. 125 АПК РФ). Кроме того, как указывают А.А. Дружинина и П.А. Паулов[1], электронное судопроизводство в арбитражных судах обеспечивает широкие возможности взаимодействия с судебной системой. Стороны получают доступ к информации о ходе дела через уникальный код, а система "Картотека арбитражных дел" открыта для ознакомления с информацией

[1] См. об этом: Дружинина А.А., Паулов П.А. Особенности реализации электронного судопроизводства в арбитражном процессе / Юридическая наука, 2021

о делах для всех пользователей, что позволяет участникам финансового рынка проверять контрагентов перед заключением сделок.

Также, отличительным примером внедрения информационных технологий в арбитражное судопроизводство, в отличие от иных видов судопроизводств в РФ, является введение в декабре 2021 в АПК РФ статьи 153.2, которая именуется как «Участие в судебном заседании путем использования системы веб-конференции». Согласно положениям данной статьи, лица, участвующие в деле, и иные участники арбитражного процесса могут участвовать в судебном заседании путем использования системы веб-конференции при условии заявления ими соответствующего ходатайства и при наличии в арбитражном суде технической возможности осуществления веб-конференции. Установление личности гражданина, его представителя или представителя юридического лица, участвующих в судебном заседании, производится путем использования системы веб-конференции, с использованием информационно-технологических средств, обеспечивающих идентификацию лица без его личного присутствия (единой системы идентификации и аутентификации, единой биометрической системы). Указанным лицам заблаговременно направляется информация в электронном виде, необходимая для участия в судебном заседании с использованием системы веб-конференции.

Участие лиц в арбитражном процессе с использованием веб-конференции является первым шагом к модернизированию отечественного судопроизводства, приводящего судопроизводство в РФ к вызовам современности и технологического процесса. Данная форма участия в процессе может быть использована и в других видах судопроизводств, исключением их которых не должно стать и уголовное судопроизводство. Так, к примеру, вполне возможно участие потерпевшего, его представителя, гражданского истца, гражданского ответчика, в некоторых случаях и свидетеля посредством веб-конференции при отсутствии необходимости явки в суд по месту жительства.

Рассматривая проблемы внедрения средств коммуникации и дистанционного взаимодействия в уголовное судопроизводство РФ, следует выделить следующее.

По мнению А.С. Петрова[1], актуальная задача модернизации уголовного судопроизводства — внедрение цифровой аудио- и видеозаписи показаний участников процесса. Это позволит повысить объективность и полноту фиксации информации, в перспективе заменив традиционные протоколы и обеспечив полностью электронный документооборот.

Также актуальным вопросом является и внедрение в уголовный процесс технологии использования дистанционных форм процессуальных действий с использованием электронных цифровых подписей вместо обычных письменных подписей. Это особенно важно в случаях, когда у лица нет возможности явиться по вызову следователя или дознавателя на место предварительного следствия. К примеру, если участник процесса проживает в другом регионе РФ.

Анализируя сложившуюся следственную практику и уровень развития информационно-коммуникационных технологий на современном этапе, мы считаем, что проведение допросов с использованием средств видео-конференц связи с применением электронно цифровой подписи, при которой лицо может выйти на связь со следователем посредством своего персонального компьютера и заверить данные им показания электронно-цифровой подписью, будет решать проблему как экономического характера, связанную с ценой уголовного судопроизводства, а также с разумностью сроков уголовного судопроизводства.

При этом, процедура получения электронной цифровой подписи лица, являющегося участником уголовного судопроизводства, в отличие от общих правил ее получения, должна быть упрощена на государственном уровне. В том числе, возможно рассмотреть возможность использования в качестве электронно-цифровой подписи функций приложения «Госключ», установка

[1] См.: Петров А.С. Перспективы применения информационных технологий в уголовное судопроизводстве / Вестник магистратуры, 2022.

которого и получение сертификата электронной подписи в которой является бесплатной.

Также, одним из дискуссионных вопросов в контексте использования современных информационных технологий для фиксации идеальных следов при расследовании преступлений является вопрос применения синхронных переводчиков[1].

Основной положительной чертой использования таких технических средств в уголовном судопроизводстве является значительная экономия времени, которое при наличии необходимости привлечения к делу переводчика, расходуется на вызов и прибытие переводчика на следственное действие или в процесс. Кроме этого, уже непосредственно при проведении процессуальных действий переводчику, привлеченному для участия в следственных действиях и судебных заседаниях требуется определённое время на перевод, как с языка судопроизводство на иностранный, так и наоборот.

Помимо вышеуказанного, электронные синхронные переводчики могут существенно облегчить процедуру перевода, например, при проведении следственных действий, не терпящих отлагательства с лицами, не владеющим языком судопроизводства: в ночное время, выходные и праздничные дни, а также в иных случаях, когда обеспечить участие переводчика не представляется возможным.

Вместе с этим, полагаем, что, несмотря на наличие большого количества положительных сторон применения таких переводчиков, имеется ряд проблемных вопросов, которые необходимо проработать перед интеграцией таких технических средств в уголовное судопроизводство.

Ключевыми вопросами являются:

---

[1] См. подробней: Швец С.В. Тактические особенности судебных действий следственного характера в условиях необходимости использования перевода // Теория и практика общественного развития. 2014. №14; Швец С.В. Криминалистическая тактика следственных и судебных действий в условиях использования перевода : автореферат дис. ... доктора юридических наук : 12.00.12 / Швец Сергей Владимирович; [Место защиты: Кубан. гос. аграр. ун-т]. — Краснодар, 2014. — 56 с..

- вопрос достоверности перевода, который будет производить техническое устройство самостоятельно при отсутствии контроля со стороны лиц, владеющих языком;

- техническая сторона указанных технических устройств, а также программного обеспечения, обеспечивающая полноту иностранных языков, доступных для перевода и синхронность такого перевода;

- порядок заверения указанных технических устройств на точность перевода со стороны лиц-носителей иностранных языков (в том числе юридические вопросы относительно того, каким статусом должен обладать заверитель: его образование, наличие определенных сертификатов и иные правовые вопросы).

При этом мы полагаем, что требования к заявителю должны соответствовать требованиям о знании иностранного языка, предъявляемым законом к переводчикам, привлекаемых к совершению нотариальных действий. В числе таких требований предлагается рассмотреть требования о наличии высшего лингвистического, филологического, педагогического образования по иностранному языку, с которого или на который осуществляется перевод; наличие у иностранного гражданина высшего лингвистического, филологического, педагогического образования по направлению "Русский язык"; наличие у лица, имеющего гражданство Российской Федерации, стажа работы более пяти лет на территории государства, в котором язык перевода является официальным; наличие у иностранного гражданина стажа работы более пяти лет на территории Российской Федерации.

Таким образом, направлениями использования информационных технологий при расследовании преступлений в сфере экономики, актуальность которых на современном этапе являются необходимыми для эффективной организации расследования, являются: информационно-справочные и аналитические системы, системы электронного документооборота и управления следственным процессом, средства коммуникации и дистанционного

взаимодействия, информационные технологии, предназначенные для фиксации следовой картины преступления, изъятие электронных носителей информации при расследовании преступлений, получение электронной информации о переписках у операторов и провайдеров, проведение допросов с использованием видеоконференцсвязи**,** иные информационные технологии для организации расследования (использование ГИС-технологий, использование нейросетей в качестве «помощника» при подготовке судебного решения для обобщения судебной практики).

ГЛАВА 2. ПРОБЛЕМЫ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ЭКОНОМИКИ

2.1. Проблемы правовой регламентации и алгоритмизации применения информационных технологий, предназначенных для фиксации следовой картины преступлений, совершенных в сфере экономики

Поскольку целью диссертации является разработка практических рекомендаций по оптимизации процесса расследования преступлений, совершенных в сфере экономики за счет эффективного применения современных информационных технологий, то в указанной главе акцентировано внимание на аспектах применения современных информационных технологий для фиксации следовой картины преступлений, а именно выделить наиболее значимые аспекты фиксации следовой картины преступлений в сфере экономики**.**

Как говорилось ранее, в эпоху развития цифровых технологий, последние постепенно с каждым днем все более тщательно интегрируются в сферу судопроизводства, в том числе уголовного, частью которого также является стадия предварительного расследования, в ходе которой следователем осуществляется собирание доказательств, являющихся основополагающими для предъявления обвинения лицам, совершившим преступления. Как известно, с учетом развивающихся информационных технологий, все более значимый объём доказательственной информации по преступлениям различных категорий, первоначально по преступлениям в сфере экономики, можно получить, проанализировав содержание переписок посредством различных мессенджеров, СМС-сообщений, установив наличие тех или иных файлов и иного содержимого электронных носителей информации (ноутбуков, мобильных телефонов, USB-накопителей), получив информацию о соединениях между абонентами с привязкой к их местоположению, произведя выемку электронных сообщений в

организации, обеспечивающей их передачу через сеть Интернет, а также проведя иные следственные действия.

В науке криминалистике такие следы, в связи с их отличием от идеальных следов, которыми являются следы, хранящиеся в памяти людей и приобретающие процессуальную форму в качестве сведений, сообщаемыми лицами в ходе допросов, а также от материальных, которыми являются изменения в элементах обстановки, возникшие в результате механического, химического, биологического и иного воздействия, выделяют в отдельную группу и именуют как электронные следы.

Как считают В.А. Мещеряков и В.Ю. Агибалов, указанная категория следов приближена к материальным следам, поскольку находится непосредственно на электронном носителе, вместе с тем, назвать указанные следы материальными нельзя, так как отсутствует неразрывная связь указанных следов с устройствами, осуществившими их запись[1]. Кроме того, такие следы являются неустойчивыми и зависят от способа их считывания. Такие следы, в юридической литературе именуются также виртуальными или цифровыми.

Однако, для более точного понимания существа рассматриваемой категории следов, следует обратиться к имеющимся в науке криминалистике определениям, данными учеными рассматриваемой категории следов. Так, профессор В.А. Мещеряков указанную категорию следов считает виртуальными следами, определяя их как «любые изменения состояния автоматизированной информационной системы, связанные с событием преступления и зафиксированные в виде компьютерной информации

[1] См. подробней: В. А. Мещеряков, А. Н. Яковлев, В. Ю. Агибалов «Расследование преступлений в сфере высоких технологий: учебное пособие» / сост. В. А. Мещеряков, А. Н. Яковлев, В. Ю. Агибалов. - Воронеж: Изд-во Воронежского гос. ун-та, 2008.

(пригодной для машинной обработки) на материальном носителе, в том числе на электромагнитном поле»[1].

Вместе с этим, обращаясь к этимологии понятия «виртуальный», следует, что оно означает «не имеющий физического воплощения или воспринимаемый иначе, чем реализован в действительности». В данной связи, на наш взгляд, формулировка данной категории следов виртуальными не является точной, поскольку указанные следы фактически имеют цифровую структуру (образованы с использованием двоичного кода), и воспринимаются на аппаратно-программном комплексе в действительности везде одинаково, а не по-разному. В связи с этим, формулировка понятия виртуальный в разрезе их применения к указанной категории следов не в полной мере применима.

В.Б. Вехов указанную категорию следов именует как электронно-цифровые следы[2]. По его мнению, электронно-цифровой след – это любая криминалистически значимая компьютерная информация, находящаяся в электронно-цифровой форме, зафиксированная на материальном носителе с помощью электромагнитных взаимодействий либо передающиеся по каналам связи посредством электромагнитных сигналов. На наш взгляд, данное определение является более подходящим к описанию исследуемой категории следов. Вместе с этим, учитывая тот факт, что вся информация, передающаяся по электромагнитным каналам связи и представленная в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, формируется с использованием цифрового (двоичного) кода, то на наш взгляд, при определении данной категории следов, стоит остановиться на таком понятии, как «электронные следы».

---

[1] См.: Иванов В.Ю. — О теоретических аспектах использования в криминалистике понятия электронно-цифрового следа // Юридические исследования. – 2020. – № 7. – С. 75 - 80. DOI: 10.25136/2409-7136.2020.7.33682

[2] См.: Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: монография. Волгоград: ВА МВД России, 2008. С. 71.

Таким образом, электронными следами следует считать любую криминалистически значимую информацию, передающуюся по электромагнитным каналам связи и представленную в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин.

Электронные следы, необходимые в доказывании по уголовным делам, возбужденным по преступлениям в сфере экономики, могут быть получены различными способами. Основными из них являются: изъятие электронных носителей информации в ходе следственных действий, допускающих изъятие объектов (например, обыск, выемка, осмотр места происшествия, а также некоторые другие). Сюда также следует отнести способ копирования интересующей следствие информации с обнаруженного в ходе следственного действия носителя информации, на иной носитель информации (при этом обнаруженный носитель информации не изымается в ходе следственного действия).

Также в практике имеет место альтернативное получение информации из другого («объективного») источника, а именно получение информации посредством следственных запросов сетевым или Интернет-провайдерам, выемка электронных сообщений в организациях, обеспечивающих передачу сообщений по сетям электросвязи, получения соединений между абонентами и абонентскими устройствами.

Кроме этого, как пишут Е.Р. Россинская и Т.А. Сааков, в качестве способа получения электронных следов следует рассматривать поиск информации с использованием технических средств, например, персонального компьютера следователя, в целях доступа на электронный сайт (страницу интересующего следователя пользователя социальной сети), где потенциально могут содержаться следы преступления[1]. После чего производится фиксация и изъятие указанной криминалистический значимой информации. При этом отличительной чертой

[1] См. подробней: Россинская Е.Р., Сааков Т.А. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров / Криминалистика: вчера, сегодня, завтра. Иркутск, 2020.

указанного вида получения электронных следов является факт нахождения интересующих следствие цифровых данных в открытом доступе. Иными словами, указанный вид получения электронных следов характеризуется как осмотр электронной страницы пользователя.

Наиболее эффективными способами получения электронных следов при расследовании преступлений является изъятие электронных носителей информации, либо же копирование с электронных носителей информации на другие электронные носители интересующей доказательственной информации.

Уголовно-процессуальный закон предписывает, что изъятие и копирование информации с электронных носителей должны осуществляться с учетом положений ст. 164.1 УПК РФ «Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий», которая введена в действие в 2018 году.

Правоотношения изъятия и копирования информации с электронных носителей до указанного времени не были отдельно регламентированы в уголовно-процессуальном законодательстве, в связи с чем, изъятие электронных носителей информации осуществлялось по общим правилам проведения тех или иных следственных действий, регламентирующих изъятие доказательственной информации в ходе проведения следственных действий. Указанная норма введена в УПК РФ в целях урегулирования указанных правовых отношениях в соответствии с современными реалиями, определяющими количество изымаемых электронных носителей информации для получения доказательственной информации по уголовному делу и ее доказательственное значение.

Вместе с этим, указанная норма в некоторых случаях создает излишние процессуальные препятствия и в некоторых случаях некую забюрократизированность процедур производства следственных действий, связанных с изъятием и копированием доказательственной информации[1].

[1] См. об этом в том числе: Кузора С.А. Проблемы участия понятых при производстве следственных действий с электронными носителями информации // Закон и право. 2021. №10.

В частности, одним из спорных вопросов, возникающих при проведении копирования, является вопрос обязательности привлечения к участию в таких следственных действиях понятых. Статья 164.1 УПК РФ сама по себе не предписывает обязательность участия понятых при производстве изъятия электронных носителей информации, однако предписывает к обязательному привлечению понятых при проведении копирования информации с электронных носителей при проведении следственных действий.

Таким образом, анализируя положения ст. 164.1 УПК РФ и нормы УПК РФ, регламентирующие общие правила проведения предварительного расследования и регламентирующие порядок изъятия предметов, имеющих доказательственное значение в ходе предварительного следствия, можно сделать вывод о том, что обеспечение участия понятых при производстве изъятия электронных носителей информации должно осуществляться следователем по общему правилу, с учетом требований, ст. 170 УПК РФ, определяющей обязательность привлечения понятых при производстве тех или иных следственных действий.

Спорный вопрос обязательности привлечения понятых к копированию информации с электронных носителей заключается как в целесообразности их привлечения, так и в эффективности их применения как института уголовно-процессуального права для удовлетворения назначения уголовного судопроизводства в части удовлетворения как публично-правовых интересов расследования, так и соблюдения интересов и прав участников уголовного судопроизводства.

Уголовно-процессуальным законодательством предусмотрено, что в качестве понятого следователем и дознавателем может быть привлечено любое незаинтересованное в исходе уголовного дела лицо, и не относящееся к категории лиц, упомянутых в ч. 2 ст. 60 УПК РФ. Каких-либо иных специальных требований к понятым УПК РФ не предусматривает, так же как и не предусматривает их для копирования информации с электронных носителей в соответствии с требованиями ст. 164.1 УПК РФ.

При таких обстоятельствах, к участию в производстве следственного действия, связанного с копированием информации с электронного носителя могут быть привлечены любые совершеннолетние лица, не являющиеся участниками судопроизводства или их родственниками, а также лицами, осуществляющими оперативно-розыскную деятельность или предварительное расследование, в числе которых могут оказаться лица, которые в силу возраста либо иных факторов могут вовсе не иметь представления о проведенных при копировании информации действиях.

В таких случаях привлечение понятых к копированию информации с электронных носителей не обеспечит в полном объёме целей их привлечения к следственному действию, а именно объективности подтверждения хода и результатов следственного действия. Так, у понятых, в качестве которых будут привлечены вышеуказанные лица, останется лишь поверхностное представление о том, какие именно действия и операции совершались в ходе копирования информации в ходе производства следственного действия, что в свою очередь не будет выступать обоснованной гарантией объективности производства такого следственного действия.

Так, обеспечение участия понятых часто бывает непростой задачей в части их поиска. Когда следственные действия планируются заранее, то обеспечить их участие проще, оперативные подразделения, осуществляющие сопровождение по уголовному делу помогают в этой части их организации. Зачастую привлекаются студенты профильных образовательных организаций, были случаи привлечения курсантов военных училищ, солдат срочной службы. Однако в условиях неотложности привлечь понятых становится намного тяжелее. В таких случаях, например, при проведении обыска, нередки случаи привлечения соседей, иных прохожих. Но как мы понимаем, если, например, следственное действие проводится в дневное время, то нередко соседями оказываются люди пенсионного возраста, так как они обычно днем находятся дома, в отличие от иных категорий граждан, занятых работой, учебой и так далее.[1]

Обращаясь к мнениям ученых, изучающих аспекты получения электронной доказательственной информации при расследовании преступлений, можно констатировать факт того, что последние также придерживаются мнения

[1] По результатам проведенного нами интервьюирования следователей. 2023 год

нецелесообразности привлечения понятых к следственным действиям, связанным с получением электронных доказательств.

По мнению В.Н. Тогулева, «необходимость поиска и привлечения понятых к следственным действиям, при которых появилась необходимость в копировании информации с электронных носителей, является нецелесообразной и создающей излишние необоснованные препятствия лицам, проводящим следственное действие»[1].

Анализируя целесообразность привлечения понятых к следственным действиям, связанным с копированием информации с электронных носителей, В.Н. Тогулев делает вывод о том, что выемка электронных носителей информации в ходе проведения следственных действий может производиться без участия понятых при участии специалиста. Вместе с этим, если в ходе следственного действия поступило ходатайство владельца изымаемого электронного носителя информации о копировании информации с изымаемого носителя на иной электронный носитель информации, то в указанном случае, следователь обязан привлечь к следственному действию не менее двух понятых. В случае, если ходатайство о копировании информации с изымаемого электронного носителя информации для следователя окажется неожиданным, то следственное действие подлежит приостановлению для отыскания понятых, что, очевидно, сказывается на время производства такого следственного действия.

Мнения исключения обязательности участия понятых при копировании информации с электронных носителей придерживается и Е.Р. Россинская, уделив указанному вопросу отдельное внимание в контексте получения электронных доказательств[2].

По ее мнению, привлечение понятых при копировании информации с электронных носителей информации является нецелесообразным при наличии

---

[1] См. об этом: Тогулев В.Н. «Понятые или техническая фиксация результатов следственных действий» / Вестник Волжского университета им. В. Н. Татищева / 2022

[2] См. подробней: Россинская Е.Р. Теория информационно-компьютерного обеспечения криминалистической деятельности. Монография. М, 2022. С 111

участвующего лица - специалиста, который обладает специальными знаниями в области информационных технологий, и, в случае возникновения каких-либо спорных вопросов, связанных с обстоятельствами произведенного копирования информации с изъятых электронных носителей информации, может быть в последствие допрошен по указанным обстоятельствам следователем или судом.

Соглашаясь с отдельными положениями, приведенными учеными, считаем, что институт понятых не применим к процессу изъятия и копирования информации с электронных носителей информации. Полагаем, что необходимость в участии понятых при производстве копирования информации с электронных носителей отсутствует, поскольку при копировании информации, сведения о скопированной информации, а именно о времени, дате, устройстве, с которого была скопирована информация, отображаются в свойствах скопированного файла. Кроме того, участвующий в ходе следственного действия понятой, вряд ли запомнит время, точные количество и содержание каждого из скопированного с электронного носителя информации файла. Такая информация в силу ее большого объема и различных характеристик, вряд ли отложится в памяти человека, даже имеющего специальные знания в сфере информационных технологий, на долгое время.

Например, при расследовании уголовного дела, возбужденного по п. «а» ч. 2 ст. 172 УК РФ в отношении организованной группы, осуществлявшей незаконные банковские операции по «обналичиванию» денежных средств через организации, оформленные на подставных лиц, следователем при производстве обыска в жилище у лица, осуществлявшего в организованной группе роль «бухгалтера» при осмотре персонального компьютера обнаружены сведения, подтверждающие факт ведения бухгалтерского учета ряду организаций, использовавшихся для «вывода» денежных средств. Там же обнаружено большое количество файлов (фотографий, видеозаписей), относящиеся к личной жизни владельца электронного носителя информации, ходатайство о копировании которой перед изъятием электронного носителя информации было заявлено лицом. При этом следователем было удовлетворено указанное ходатайство в части копирование вышеуказанной личной информации, не представляющей для следствия интереса, на другие электронные носители информации, предоставленные законным владельцем изымаемых электронных носителей информации. При проведении копирования присутствовали понятые и специалист, которому непосредственно и было поручено копирование. Ввиду

большого количества копируемой информации, она была перекопирована на несколько предоставленных электронных носителях. Все эти носители были указаны в протоколе. Однако, по понятным причинам, запомнить количество скопированных файлов и количество носителей, на которые проводилось копирование, никто от понятых не требовал. При изъятии электронного носителя информации было лишь обращено внимание понятых на наличие документов интересующих следствие организаций. [1]

Таким образом, считаем, что цель фиксации хода и результатов следственного действия, в ходе которого производится копирование информации с электронных носителей, в меньшей степени может быть достигнута посредством привлечения понятых, однако формальная в силу закона обязательность их привлечения, создает дополнительные трудности к подготовке и производству ряда таких следственных действий.

Касаясь аспекта обеспечения прав участников уголовного судопроизводства, следует обратить внимание на то, что при наличии претензий участников уголовного судопроизводства, в том числе со стороны владельцев изъятых носителей информации, относительно полноты проведенного копирования информации, которая необходима ему для ведения законной деятельности, то указанный вопрос может быть решен посредством заявления ходатайства следователю в ходе предварительного следствия, либо в суде. Целесообразно закрепить и регламентировать в законе механизм предоставления законному владельцу изъятого электронного носителя информации дополнительной возможности копирования с изъятого электронного носителя той информации, которая необходима ему для ведения законной деятельности, соответственно исключая возможность копирования при наличии обстоятельств, указанных в п.3 ч.1 ст. 164.1 УПК РФ, то есть если на электронных носителях информации содержится информация, полномочиями на хранение и использование которой владелец электронного носителя информации не обладает, либо которая может быть использована для совершения новых

[1] Из практики работы Следственной части по расследованию организованной преступной деятельности УМВД России по Калининградской области за 2021 г.

преступлений, либо копирование которой, по заявлению специалиста, может повлечь за собой ее утрату или изменение.

Как известно, процесс привлечения к производству следственного действия понятых, значительно увеличивает время подготовки следственного действия. Несомненно, в конкретно определенных законом случаях, как, например, обыск, их присутствие бесспорно является необходимым, поскольку их участие гарантирует обеспечение прав и интересов граждан, в отношении которых проводятся следственные действия, а также объективность производства самого следственного действия. Вместе с тем, с учетом постоянно развивающихся цифровых технологий и развитых средств вычислительной техники, способных более достоверно фиксировать факты объективной реальности, следует постепенно их использовать и адаптировать применительно к процессу получения доказательств и законодательно регламентировать их использование. В частности, при производстве следственных действий, связанных с получением информации с электронных носителей, следует более активно использовать технические способы фиксации хода и результатов следственных действий, и постепенно законодательно уходить от обязательного участия понятых, в случаях, когда этого не требует тактическая необходимость.

Полагаем, что вопрос о привлечении понятых должен решаться следователем в зависимости от складывающейся следственной ситуации. В тех случаях, когда у следователя возникнет необходимость в фиксации определенных фактов именно человеком, например в случае противодействия следствию в процессе изъятия носителей, или, например, в случаях обязательного участия понятых в силу закона, понятые могут быть им привлечены по собственной инициативе.

В настоящее время, не ставим под сомнение необходимость в обязательном участии понятых, в случаях, предусмотренных ч. 1 ст. 170 УПК РФ, то есть в случаях их обязательного участия в следственных действиях, вместе с тем, считаем необходимым рассмотреть возможность ухода от обязательного

привлечения понятых при копировании информации с электронных носителей информации при производстве следственных действий, не требующих обязательного участия понятых.

Не менее спорным вопросом в контексте рассмотрения аспектов проведения следственных действий, в ходе которых производится изъятие и копирование информации с электронных носителей информации, является вопрос участия специалиста при проведении указанных следственных действий[1].

Представляется спорным установленное в ст. 164.1 УПК РФ законодательное требование о необходимости обязательного привлечения к участию в следственных действиях, в ходе которых осуществляется изъятие электронных носителей информации, специалиста.

Как следует из определения электронного носителя информации, закрепленного в п. 3.1.9 ГОСТ 2.051-2013. «Межгосударственный стандарт. Единая система конструкторской документации. Электронные документы. Общие положения», «электронным носителем информации является такой материальный носитель, который используется для записи, хранения и воспроизведения электронной информации, обработка которой происходит с помощью средств электронно-вычислительной техники».

Анализом закрепленного в ГОСТ определения, можно сделать вывод о том, что оно подразумевает под собой любой материальный носитель, на котором записана электронная информация, вне зависимости от ее размера, технической сложности и иных характеристик. Электронным носителем информации является как оптический диск, так и сервер, обеспечивающий работоспособность и хранение информации целой организации. Учитывая тот факт, что электронные носители информации, которыми являются, в том числе смартфоны, ноутбуки, usb-накопители и иные, находятся повсеместной и ежедневной эксплуатации

[1] См.: Абсатаров, Р. Р. Правовые проблемы изъятия электронных носителей информации и получения копий с них / Р. Р. Абсатаров // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. – 2023. – № 1(71). – С. 25-28. – EDN HEEXRC.

обычными пользователями, то, соответственно, уровень пользования такой компьютерной техникой и общих знаний относительно процесса изъятия электронных носителей информации и копирования с них информации, имеющийся у подавляющего большинства пользователей, которыми являются и сотрудники правоохранительных органов - следователи, дознаватели, оперативные сотрудники, на наш взгляд, соответствует достаточной квалификации для производства самостоятельного изъятия стандартных электронных носителей информации или копирования с них доказательственно-значимой информации. В частности, в данную группу могут входить оптические диски, usb-носители, персональные компьютеры, мобильные телефоны (смартфоны).

Вместе с этим, закрепленный в УПК РФ порядок изъятия электронных носителей информации не предусматривает возможности их изъятия без участия специалиста, что на практике довольно часто усложняет процесс расследования преступлений без оправданной на то необходимости.

Результатами анкетирования сотрудников следственных подразделений относительно наличия у них общих знаний информационных технологий и навыков изъятия базовых носителей информации, установлено, что у 90 % опрошенных следователей в дипломе о высшем образовании предусмотрены дисциплины «Информатика», «Основы ИКТ». 87 % респондентов заявили, что имеют базовые навыки изъятия электронных носителей информации и только 5 % опрошенным сотрудникам следственных органов требуется участие специалиста при изъятии базовых электронных носителей информации (мобильные телефоны, ноутбуки и иные). Более подробно результаты анкетирования представлены в Приложении 2 настоящего исследования.

Ученые–криминалисты, анализировавшие проблемы получения доказательственной информации с электронных носителей, пришли к различным выводам относительно оправданной необходимости участия специалиста при производстве изъятия электронных носителей информации. Так, например, Е.Р. Россинская считает, что «участие специалиста должно быть обязательным в случаях, когда требуется произвести изъятие компьютерной информации

непосредственно с электронного носителя информации (персонального компьютера, планшета, мобильного телефон и т.д.), либо в случаях, когда требуется изъятие информации, находящейся на удаленных серверах, а не на самом электронном носителе информации»[1].

Некоторые ученые считают необходимым закрепить на законодательном уровне случаи, при которых участие специалиста будет являться необязательным[2].

По мнению С.В. Зуева, «современные информационные технологии являются вполне простыми в обращении. Их использование в большинстве своем не требует каких-либо специальных умений и знаний по их применению»[3].

Аналогичного мнения придерживается С.Б. Россинский, опираясь на то, что обладая «базовыми специальными знаниями и умениями обращения с цифровой техникой, следователь при обращении с ней вполне может обойтись без помощи специалиста»[4].

Проведя анализ результатов интервьюирования следователей, и придерживаясь ситуационного подхода в криминалистике, считаем, что привлечение специалиста к участию в следственных действиях, связанных с изъятием или копированием информации с электронных носителей, должно определяться следователем по собственной инициативе в порядке,

---

1 См. подробней: Россинская Е.Р. Теория информационно-компьютерного обеспечения криминалистической деятельности. Монография. М, 2022. С 111

[2] См.: Закомолдин, А. В. Проблемы определения критерия необходимости в привлечении специалиста при изъятии электронных носителей информации в уголовном процессе России / А. В. Закомолдин // Вектор науки Тольяттинского государственного университета. Серия: Юридические науки. – 2019. – № 1(36). – С. 9-13. – EDN IVKPSY.

[3] См. об этом: Зуев С. В. Развитие информационных технологий в уголовном судопроизводстве: моногр. М. : Юрлитинформ, 2018. 248 с.

4 См.: Россинский С.Б. Следственные действия: монография. М.: Норма, 2018. № 6. С. 118.

предусмотренном ст. 168 УПК РФ исходя из скалывающейся следственной ситуации.

Законодательное закрепление обязательности привлечения специалиста к участию во всех следственных действиях, в ходе которых производится изъятие электронных носителей или копирование с них информации, безусловно, не является в настоящее время обоснованным правовым механизмом, призванным гарантировать соблюдение прав и законных интересов граждан-владельцев изымаемых электронных носителей информации или тех носителей информации, с которых непосредственно производится копирование информации.

Так, к примеру, в следственных ситуациях, в которых имеется необходимость изъятия технически сложных электронных носителей информации, либо же копирования с них информации на другие носители, к примеру, информации с удаленных серверов либо иных электронных носителей информации, специальных знаний об изъятии информации с которых у следователя недостаточно, ввиду чего в случае изъятия или копирования информации с таких электронных носителей информации, следователь в любом случае прибегнет к помощи специалиста и привлечет его к участию в следственных действиях самостоятельно.

Исключение требования об обязательности привлечения специалиста, послужит шагом к преодолению излишней забюрократизированности требований уголовно-процессуального законодательства, в частности фактов, привлечений сотрудников экспертных подразделений к участию в следственных действиях, где фактически познаний, имеющихся у следователя, дознавателя или оперативного сотрудника, вполне достаточно для грамотного изъятия электронного носителя информации, и применения каких-либо специальных знаний в этой области не требуется.

При этом, права и законные интересы лиц, у которых будет производиться изъятие или копирование информации с электронных носителей информации, на участие квалифицированного специалиста в таких следственных действиях, защищают уже действующие в настоящее время нормы права. Так, в случае несогласия участвующих в следственном деле лиц с уровнем компетенции следователя, дознавателя или оперативного сотрудника, осуществляющих изъятие или копирование информации с электронных носителей информации, уголовно-процессуальным законом, в ст. 57 УПК РФ, в качестве гарантий прав стороны защиты, закреплено положение, согласно которому «стороне защиты не может быть отказано в удовлетворении ходатайства о привлечении к участию в производстве по уголовному делу специалиста для разъяснения вопросов, входящих в его профессиональную компетенцию».

Таким образом, в случае наличия сомнений в компетенции должностного лица, проводящего следственное действие, связанной с наличием достаточных знаний и умений по изъятию и копированию информации с электронных носителей, вопрос о привлечении специалиста к производству следственного действия может быть решен в порядке заявления стороной зашиты соответствующих ходатайств.

Рассматривая способы получения электронной доказательственной информации, не связанные с изъятием и копированием информации с электронных носителей, в ходе производства по уголовным делам, важно выделить такие следственные действия как «выемка электронных сообщений в организациях, обеспечивающих передачу сообщений по сетям электросвязи» и «получение соединений между абонентами и абонентскими устройствами», а также направление следственных запросов интернет и сетевым провайдерам. Указанные следственные действия связаны с получением электронной доказательственной информации из альтернативных объективных источников, а именно с обращением в организации, обеспечивающие передачу сообщений по

сетям электросвязи, к сетевым или Интернет-провайдерам, с целью истребования доказательственной информации, хранящейся на их серверах.

Практика получения такой доказательственной информации в настоящее время имеется. Российские организации, обеспечивающие передачу сообщений по сетям электросвязи, к числу которых можно отнести ООО «ВК» (социальная сеть vk.com, почтовый сервис mail.ru), ООО «Яндекс» и иные, в ответ на следственные запросы предоставляют интересующую следствие информацию (например, сведения о местонахождении устройств при выходах в сеть интернет по ip-адресам). Кроме того, в российских организациях, обеспечивающих передачу сообщений по сетям электросвязи, по решению суда может быть произведена выемка сообщений электронной почты, переписки в социальных сетях.

Так, к примеру, при расследовании уголовного дела, возбужденного по п. «а» ч. 2 ст. 194 УК РФ по факту уклонения от уплаты таможенных платежей, после получения соответствующего судебного постановления, разрешающего выемку электронных сообщений электронной почты домена @mail.ru в ООО «ВК» проведена выемка электронных сообщений, подтверждающих направление таможенному декларанту документов, содержащих ложные сведения относительно наименования товара (по ТН ВЭД ЕАЭС), ставки уплаты платежей по которым ниже фактически применяемых в отношении поставляемой продукции, которые в дальнейшем внесены в таможенные декларации на товары, в целях уклонения от уплаты таможенных платежей [1].

Вместе с этим, при проведении выемки сообщений электронной почты, переписки в социальных сетях в организациях, обеспечивающих передачу сообщений по сетям электросвязи можно столкнуться с проблемой, связанной с истечением срока хранения сообщений на сервере такой организации. На практике, организации, обеспечивающие передачу сообщений по сетям электросвязи, хранят на серверах сообщения пользователей, которые сохранены

[1] Из практики работы отдела дознания Северо-Западной оперативной таможни Северо-Западного таможенного управления за 2024 г.

(не удалены) из их аккаунтов. В случае удаления таковых, организации, обеспечивающие передачу сообщений по сетям электросвязи, хранят такие сообщения на протяжении 6-ти месяцев с момента их удаления.

Такая практика хранения удаленных сообщений основана на положениях ст. 64 Федерального закона от 7 июля 2003 г. N 126-ФЗ "О связи"[1], а также положениями пункта 5 Правил хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи, утвержденных Постановлением Правительства Российской Федерации от 12 апреля 2018 г. N 445[2].

Таким образом, наибольшая эффективность в производстве данного следственного действия возникает в случае расследования преступлений, совершенных не ранее 6 месяцев до момента их выявления и возбуждения уголовного дела. Эффективность проведения такого следственного действия возрастает также в случае, если переписка или часть переписки на изъятом электронном носителе информации в ходе обыска или иных следственных действий по уголовному делу, удалены.

В целях наиболее эффективной фиксации электронных следов на первоначальном этапе расследования преступлений в сфере экономики, разработан алгоритм первоначальных следственных действий при расследовании преступлений в сфере экономики, включающий комплекс следственных действий как направленных на отыскание электронных носителей информации, которые могут содержать интересующие следствие данные, так и получение электронных следов из альтернативных источников.

Действия следователя на первоначальном этапе расследования преступлений в сфере экономики, при которых требуется получение электронной

---

[1] Федеральный закон от 7 июля 2003 г. N 126-ФЗ "О связи" (с изм. и доп. от 04.08.2023).

[2] Постановление Правительства РФ от 12 апреля 2018 г. N 445 "Об утверждении Правил хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи".

доказательственной информации, по нашему мнению, должны выглядеть следующим образом:

- Определение круга технических устройств, абонентских номеров, электронных почтовых ящиков, аккаунтов в мессенджерах, используемых интересующими следствие лицами, где может быть обнаружена криминалистически значимая информация. Это необходимо выполнить посредством направления запросов операторам, в банки, изучения текстов договоров (изучение реквизитов организаций), изучением сведений, указанных в протоколах допросов (актах опросов) и иные способы. В этих целях в том числе необходимо алгоритмизировать на государственном уровне вопрос взаимодействия следственных (иных правоохранительных органов) с операторами связи и организациями, обеспечивающими передачу сообщений по сетям электросвязи – в целях наиболее быстрого получения следственными органами абонентских номеров, электронных почтовых ящиков в отношении интересующих лиц. Также возможно создание единых обновляющихся баз данных.

- Проведение обысков и выемок в целях изъятия электронных носителей информации (либо копирования информации с электронных носителей в ходе следственных действий). При этом, предпочтение отдается изъятию электронных носителей информации, поскольку в ходе обыска или выемки произвести полноценное копирование информации, в том числе удаленных файлов, данных или переписок, например, с мессенджеров, не всегда представляется технически возможным, а требует назначения исследований и экспертиз.

- Получение судебных решений и направление их уполномоченным представителям компаний, обеспечивающих передачу сообщений, звонков по сетям электросвязи в целях получения переписок, сохраненных или удаленных с электронных почтовых ящиков (мессенджеров), получения информации о

соединениях между абонентами и абонентскими устройствами. При необходимости также следует рассмотреть вопрос и направления международных запросов об оказании правовой помощи.

- Истребование выписок по расчетным счетам организаций и граждан, являющихся фигурантами преступлений – для их комплексного анализа в совокупности с иными собранными доказательствами.

Тем не менее, имеется проблема производства выемки электронных сообщений в иностранных организациях, обеспечивающих передачу сообщений по сетям электросвязи (Gmail, Telegram и др.)[1]. Указанные проблемы обусловлены как ограниченными сроками хранения электронных сообщений на серверах компаний установленных в соответствиями с требованиями законодательств иностранных государств и международным правом, а также так называемым «сквозным шифрованием», при котором компания вовсе не хранит сообщения передаваемые в чатах, а также трудностями, связанными с обращением в компетентные органы иностранных государств с запросом об оказании правовой помощи в порядке ст. 453 УПК РФ. Трудности, связанные с обращением в компетентные органы иностранных государств с запросами об оказании правовой помощи обусловлены как длительностью процедуры направления и истребования в последующем от них информации, так и риском неполучения необходимой информации. Так, компетентные органы иностранных государств в соответствие с заключенными с Российской Федерацией международными договорами или международными соглашениями могут отказать в оказании правовой помощи по различным основаниям (например, если расследуемое в РФ деяние не является преступлением по законодательству

[1] См. об этом: Вехов В. Б., Васюков В. Ф. Получение компьютерной информации от организаторов ее распространения в сети Интернет при расследовании преступлений // Российский следователь. 2018. № 3. С. 11-15; Берова Д.М. Особенности использования компьютерной информации из сети «Интернет» при расследовании преступлений в Российской Федерации // Пробелы в российском законодательстве. 2020. №2; Никитина Е.В., Раменская В. С. Проблемы законодательного регулирования следственного действия, направленного на получение доступа к электронным сообщениям // Российское право: образование, практика, наука. 2022. № 2.

иностранного государства, либо предоставление интересующей информации может нанести ущерб иностранному государству и др.). В таких случаях, наибольшую эффективность приобретает изъятие электронного носителя информации, а при отсутствии на таковых интересующей следствие информации, назначение и проведение компьютерно-технических судебных экспертиз.

Рассматривая проблемы правовой регламентации применения информационных технологий для фиксации электронных следов можно сделать следующие выводы, связанные как с совершенствованием производства изъятия электронных носителей информации, копирования с них доказательственно-важной информации, так и с необходимостью использования альтернативных способов получения электронной доказательственной информации.

В настоящее время в связи с повсеместно распространяющимся технологическим прогрессом, использование информационных технологий в сфере расследования преступлений является одних из важных направлений как для криминалистической составляющей совершенствования процесса расследования преступлений, так и для законодательной регламентации их использования в указанной сфере.

В последние годы можно констатировать, что законодателями и правоприменителями все большее внимание уделяется совершенствованию использования информационных технологий. Подтверждением вышесказанного является как совершенствование уголовно-процессуального законодательства, устанавливающего новые формы производства следственных действий, связанных с фиксацией как идеальных и материальных следов, так и совершенствование криминалистических средств, позволяющих их фиксировать в ходе расследования.

Обращаясь к процессуальному – законодательному вопросу совершенствования уголовно-процессуального законодательства, можно отметить вступившие в январе 2022 года в законную силу изменения в

ст. 189 УПК РФ, введенные в декабре 2021 года, позволяющие проводить допросы, очные ставки и предъявление для опознания с использованием систем видео-конференц-связи.

Практика применения указанной нормы права в настоящее время не так велика, вместе с этим она постепенно начинает реализовываться в предварительном расследовании. Как отмечает К.С. Плахота, в настоящее время имеется потребность правоохранительных органов в производстве следственных действий дистанционно, что обусловлено, например, необходимостью предоставить дополнительные гарантии безопасности свидетелям и лицам, потерпевшим от преступлений, а также экономии финансовых затрат при проведении следственных действий между лицами, находящимися на достаточном удалении друг от друга[1].

Вместе с этим, несмотря на то, что норма права, регламентирующая порядок проведения следственных действий с использованием видео-конференц-связь введена в уголовное законодательство в декабре 2021 года (в законную силу вступила в январе 2022 года), на практике указанный процессуальный механизм не выработал себя в полной мере, также как в теории уголовного процесса и криминалистики у ученых нет пока однозначных ответов на вопросы, касающиеся организации проведения таких следственных действий, а также тактики их проведения.

О необходимости и актуальности использования систем видео-конференц связи в науке уголовного процесса и криминалистики, а также на практике говорят уже давно[2]. В частности, как следует из анкетирования, результаты

---

[1] См. подробней: К.С. Плахота Использование видео-конференц связи при расследовании преступлений. Вестник Краснодарского университета МВД России, Краснодар, 2021. С. 94-96.

[2] См. об этом: Плахота К.С. Использование видео-конференц-связи при расследовании преступлений // Вестник КРУ МВД России. 2021. №3 (53); Фарафонова О.А. Использование видео-конференц-связи в уголовно-процессуальном производстве // Научный вестник ОрЮИ МВД России им. В. В. Лукьянова. 2024. №4 (101); Василькова Е.В. Проблемные аспекты

которого приведены К.С. Плахотой, согласно которому еще в 2021 году, а именно до введения в действие ст. 189. 1 УПК РФ, 50 следователей правоохранительных органов, которым был задан вопрос о наиболее предпочтительных для проведения с помощью системы видео-конференц-связи следственных действия, сообщили следующее. Так, наиболее предпочтительным следственным действием является допрос - (79% опрошенных сотрудников отдали предпочтение данному следственному действию); очная ставка (36% сотрудников), а также опознание (36% сотрудников). Кроме этого, 21 процент опрошенных упомянул следственный эксперимент и столько же проверку показаний на месте.

Однако в декабре 2021 введена и в настоящее время постепенно применяется указанная норма права, регламентирующая допросы, очные ставки и предъявление для опознания с использованием систем видео-конференц-связи.

Ввиду отсутствия широкой практики применения указанной нормы права, в науке криминалистики и уголовно-процессуального права в настоящее время отсутствуют теоретические рекомендации, позволяющие алгоритмизировать процесс проведения указанных следственных действий, и, в связи с чем, на практике у следователей, при возникновении следственных ситуаций, связанных с необходимостью проведения следственных действий с участниками процесса, проживающими на значительном удалении от места производства предварительного следствия, возникают вопросы, связанные с процедурой и тактикой производства таких следственных действий.

Анализируя положения ст. 189.1 УПК РФ, порядок проведения таких следственных действий представляется следующим. Следователь, в производстве

применения видео-конференц-связи при расследовании преступлений, предусмотренных статьёй 193.1 Уголовного кодекса Российской Федерации // Вестник Уральского юридического института МВД России. 2022. №4 (36); Афанасьева С. И., Добровлянина О. В. Правовое регулирование производства следственных действий с использованием видео-конференц-связи по действующему УПК РФ // Ex jure. 2022. №4.

которого находится уголовное дело, направляет следователю, дознавателю или в орган дознания по месту нахождения свидетеля, потерпевшего или как указано в законе «лица, участие которого в следственном действии признано необходимым» отельное поручение об организации участия данного лица в следственном действии. После обеспечения участия указанного лица, следственное действие проводится с использованием систем видео-конференц связи государственных органов, осуществляющих предварительное расследование. При этом, фактически в производстве следственного действия фактически участвуют два следователя: один по месту производства предварительного расследования, который по сути является ведущим лицом производства следственного действия, а именно который задает вопросы, предъявляет для опознания лиц, предметы, фиксирует ход и результаты следственного действия, ведет протокол следственного действия. Второй следователь (дознаватель или сотрудник органа дознания) находится по месту нахождения лица, участие которого в следственном действии признано необходимым, который обеспечивает участие в ходе следственного действия такого лица, обеспечивает разъяснения последнему его процессуальных прав, а также составляет по результатам следственного действия процессуальный документ – подписку о разъяснении прав и порядка процессуального действия, а также фиксирует в данной подписке замечания о дополнении и уточнении протокола следственного действия, оглашенного следователем по месту проведения предварительного следствия, которым непосредственно и был составлен протокол.

Безусловным плюсом возможности проведения следственных действий с использованием видео-конференц-связи является возможность непосредственно следователю, в производстве которого находится уголовное дело лично задавать вопросы допрашиваемому лицу и, соответственно, непосредственно сразу

формулировать возможные «вытекающие» вопросы исходя из ответов допрашиваемого лица. Безусловно, такой порядок производства допроса с тактической стороны в существенно лучшую сторону отличается от классического направления поручения следователю в другой регион в порядке ч.1 ст. 152 УПК РФ, при котором следователем, например, направляется поручение о допросе лица в другой регион РФ и прилагается список вопросов указанному лицу. В таком случае следователь следственного органа по месту нахождения допрашиваемого лица, хоть и задаст все приведенные следователем, в производстве которого находится уголовное дело, вопросы, однако, не владея в полном объёме материалами расследуемого уголовного дела, не сможет сформулировать важные для конкретной следственной ситуации «вытекающие» вопросы, зафиксировать ответы на которые, к примеру, тактически целесообразно было бы непосредственно сразу в ходе проведения указанного допроса.

Так, к примеру, при расследовании уголовного дела, возбужденного по ч. 1 ст. 196 УК РФ по факту преднамеренного банкротства следователем направлено отдельное поручение в Следственное управление по ЦАО г. Москвы о допросе свидетеля С. Получив результаты исполненного поручения, исходя из установленной информации, возникла необходимость в производстве дополнительного допроса указанного свидетеля. В результате чего в вышеуказанный следственный орган направлено поручение о производстве дополнительного допроса свидетеля С. с приложением необходимых дополнительных допросов, необходимых к выяснению[1].

Кроме того, несомненно, огромным плюсом в контексте применения видео-конференц-связи при производстве следственного действия является закрепленная в законе обязательность видеозаписи производства таких

[1] Из практики работы Следственной части по расследованию организованной преступной деятельности СУ УМВД России по Калининградской области за 2022 г.

следственных действий. Безусловно, законодательно закрепленная обязательность применения видеозаписи при производстве следственных действий служит дополнительным гарантом объективности производства такого следственного действия и, в частности, механизмом, позволяющим нивелировать ситуации, при которых участник следственного действия, в особенности, находящийся не по месту производства предварительного следствия, а по месту нахождения лица, участие которого необходимо, решит отказаться от данных в ходе следственного действия показаний, либо сошлется на неточность составления протокола, неправильное отражение в протоколе данных им показаний, ссылаясь также на то обстоятельство, что с изготовленным протоколом он не знакомился, а протокол оглашался следователем. В таких случаях, следователь, суд и иные участники процесса смогут обратиться к видеозаписи такого следственного действия и устранить указанные сомнения или попытку противодействовать расследованию.

Ю.Н. Пономаренко в своих тезисах делает вывод о том, что видеозапись является «важным доказательством подтверждённой информации», однако, считает, что в законе не конкретизировано, каким образом она должна осуществляться и кто из участников следственного действия должен быть в поле зрения камеры. Также он считает, что целесообразно в законе закрепить обязательность видеосъёмки в четырех положениях: «запись экрана, ориентирующая съёмка с захватом всего происходящего в помещении, съёмка конкретного места с видом на экран технического средства и лицо, в отношении которого проводится действие, а также окружающую обстановку вокруг данного лица»[1]. Такую столь трудоемкую с технической стороны вопроса процедуру видеозаписи, автор обосновывает «неблагонадежностью» следователей, которые

[1] См. об этом: Пономаренко Ю.Н. «Особенности производства допроса, очной ставки, опознания путём использования видео-конференц связи: актуальные проблемы и пути их решения», Международный научный журнал «Вестник Науки» № 6 (51) Т.1, Уфа, 2022

при получении «невыгодной», но правдивой информации при производстве следственного действия, могут отключить видеозапись, сославшись на технический сбой.

Не соглашаясь с таким мнением, считаем, что вопрос оценки таких доказательств в спорных ситуациях с позиции допустимости, также согласно УПК РФ, является прерогативой следователя и суда. Суд, в частности при отсутствии видеозаписи такого следственного действия и отсутствии подтверждения данных показаний участником уголовного судопроизводства вправе признать такое доказательство недопустимым, поскольку нарушен порядок проведения следственного действия, в частности, отсутствует видеозапись. Несомненно, видеозапись является важным гарантом и подтверждением фактического хода и результатов следственного действия.

Однако, в контексте рассмотрения целей введения указанной нормы права, направленной на преодоление процессуальных трудностей, оптимизации финансовой стороны проведения следственных действий с участниками, проживающими на значительном удалении от места производства расследования и, тем самым, соблюдения разумного срока расследования, введение дополнительных обязательных требований по осуществлению видеозаписи всего хода следственного действия с использованием видео-конференц-связи с четырех различных положений, является необоснованно трудновыполнимым требованием, практически не осуществимым на практике в большинстве следственных органов РФ и фактически не отвечающим требованиям безусловной необходимости для всех следственных действий, произведенных с использованием видео-конференц-связи.

Фактически, на практике такие следственные действия производятся с использованием программ ведомственной видео-конференц-связи, используемых в правоохранительных органах в большинстве своем в административных целях

– для проведения дистанционных совещаний, конференций. Программа представляет собой аналог всеми известных программ «Skype», «Zoom» и иных, позволяющих производить устанавливать видеосвязь с фронтальной (веб-камеры) на ПК собеседников. В органах внутренних дел, в частности, используется программа СВМС-М, которая также обладает вышеперечисленным функционалом. Хочется также дополнить, что указанная программа, наряду с многими другими программами обладает функцией «записи экрана». То есть на экране фактически будет иметься видеозапись как с веб-камеры на ПК по месту производства предварительного следствия, так и с веб-камеры на ПК по месту нахождения участника уголовного процесса (на удалении).

*Так, к примеру, при расследовании уголовного дела, возбужденного по ч. 4 ст. 159 УК РФ по факту хищения бюджетных денежных средств руководителем ООО «Д**-***» посредством представления заказчику по контракту документов, содержащих заведомо ложные сведения относительно факта поставки на объект оборудования, следователем проводилась очная ставка с использованием систем видео-конференц-связи с использованием программы ведомственной связи СВКС-М. При этом видеозапись производилась посредством этой же программы, как следователем, находящимся по месту производства предварительного следствия, так и по месту нахождения второго участника следственного действия. Фиксировалось изображение с веб-камер по двум местам производства очной ставки* [1].

Безусловно, важной рекомендацией по производству видеозаписи следственных действий с использованием видео-конференц-связи является расположение допрашиваемых лиц (участников следственного действия) перед веб-камерой, которая осуществляет запись, а также применение функции «записи экрана» как на персональном компьютере по месту производства предварительного следствия, так и с веб-камеры на персональном компьютере по

[1] Из практики работы Следственной части по расследованию организованной преступной деятельности СУ УМВД России по Калининградской области за 2022 г.

месту нахождения участника уголовного процесса (на удалении). Что будет являться дополнительной гарантией объективности производства такого следственного действия и предотвратит факт возможной технической неисправности устройств видеозаписи.

Изучая особенности использования видео-конференц-связи в различных отраслях отечественного и зарубежного права, можно отметить тенденцию к постепенной актуализации использования видео-конференц-связи в целях обеспечения дистанционной явки лиц для участия в судебном заседании. При этом подключение указанных лиц к видео-конференции в судебном заседании производится без фактического прибытия в какие-либо государственные органы.

Такую концепцию обеспечения доступа к участию в следственных действиях можно предусмотреть и в уголовном судопроизводстве, в том числе и в ходе досудебного производства.

С учетом развития удаленных средств участия в следственных действиях, например, обеспечения участников уголовного процесса электронно-цифровыми подписями, представляется возможным проведение следственных действий с использованием видео-конференц-связи (допросов, очных ставок) в отсутствие явки лица, проживающего на значительном отдалении от органа предварительного следствия, в следственный орган по месту его жительства.

Механизм производства таких следственных действий может реализовываться по аналогии с арбитражным судопроизводством, в котором уже имеется механизм дистанционного участия участников в судебных заседаниях путем использования системы веб-конференции при условии заявления ими соответствующего ходатайства и при наличии в арбитражном суде технической возможности. Установление личности гражданина, участвующего в таком судебном заседании проводится путем использования системы веб-конференции, с использованием информационно-технологических средств, обеспечивающих

идентификацию лица без его личного присутствия (единой системы идентификации и аутентификации, единой биометрической системы).

Такой способ организации участия в следственном действии участников процесса возможен в случаях, при которых привлеченный участник процесса не окажет противодействия в ходе его производства и является лицом, которое занимает активную позицию по уголовному делу. Например, активно дает изобличающие показания или не зависимо от иных участников процесса дает показания, объективность которых не вызывает сомнения.

В рамках расследования преступлений в сфере экономики, многие участвующие лица — сотрудники организаций-контрагентов, иные фигурирующие в ходе экономической деятельности лица (таможенные декларанты, страховые агенты и арбитражные управляющие) — добровольно предоставляют исчерпывающие правдивые показания.

В вышеописанных случаях, следователь может в зависимости от складывающейся следственной ситуации, обойтись без тактических приемов, эффективных только при личном присутствии в следственном отделении. Ввиду чего допросы указанных лиц, а также очные ставки с их участием могут быть проведены удаленно, с использованием видео-конференц-связи и электронной подписи, в отсутствие необходимости явки указанных лиц по месту производства следственного действия.

Решение о проведении следственных действий с дистанционным участием допрашиваемого лица в любом случае должно приниматься следователем, исходя из тактической целесообразности и складывающейся следственной ситуации.

Как известно, видеосъёмка, фотосъёмка, аудиозапись является второстепенным средством фиксации хода и результатов следственных действий. Основным средством фиксации хода и результатов следственного действия – является протокол следственного действия, который составляется следователем с учетом всех требований ст. 166 УПК РФ.

Современные технические средства играют важную роль в упрощении повседневной жизни человека, оптимизации времени и достижении качественных результатов. В расследовании уголовных дел также используются технические средства, которые направлены как на объективную фиксацию хода и результатов следственных действий, так и на уменьшение человеческого фактора, как элемента субъективизма.

Положительные аспекты применения фотографии при проведении следственных действий при расследовании преступлений совершенных в сфере экономики:

- Наглядность;

- Возможность предоставления фотографий в цифровом виде для проведения дальнейших исследований и экспертиз

- уменьшение человеческого фактора, как элемента субъективизма.

Цифровая фотография вносит значительные изменения в методику фотосъемки. Ключевые преимущества заключаются в возможности мгновенного просмотра результата фотографирования, позволяющего сразу оценить результат; в возможности редактирования параметров снимка (экспозиция, контраст, цвет и другие) после съемки; использование разнообразных эффектов и фильтров для творческой обработки; надежное хранение и архивирование фотографий на электронных носителях, гарантирующее их сохранность на длительный срок.

Безусловно, все вышеперечисленные характеристики цифровой фотографии являются ее преимуществом, позволяющим хранить объективную информацию, отражающую факт проведения следственного действия и фиксируя ход и результаты его проведения.

При производстве следственных действий следователи зачастую прибегают к помощи специалистов, обладающих специальными познаниями в области фотографии, которые в зависимости от следственной ситуации и тактической стороны производства конкретного следственного действия, могут применить

различные приемы фотосьемки и различные ее виды[1]. Касаясь тактических особенностей расследования преступлений в сфере экономики, можно отметить, что привлечение специалиста в целях производства фотосьемки при производстве следственных действий не является исключением.

Панорамная фотосъемка - это метод фотографии, который позволяет создавать фотографии, изображающие обширные панорамы. В зависимости от направления и ориентации объектива, можно выделить следующие виды панорамной фотосъемки:

* Круговая: при этом методе камера перемещается вокруг точки, чтобы запечатлеть окружающую среду в полном обзоре.

* Линейная горизонтальная: камера перемещается горизонтально, чтобы запечатлеть панораму слева направо.

* Линейная вертикальная: камера перемещается вертикально, чтобы запечатлеть панораму снизу вверх.

* Комплексная (горизонтально-вертикальная): при этом методе камера перемещается и в горизонтальном, и в вертикальном направлении, чтобы запечатлеть обширную панораму[2].

В цифровую эпоху панорамная фотосъемка может быть реализована с помощью специальных компьютерных программ, таких как Panorama Maker, Realviz Stitcher, Panorama Factory и т.д. Эти программы автоматически составляют панораму из отдельных фотоснимков и позволяют распечатать ее на фотопринтере.

---

[1] См. подробнее: Дмитриев А.В., Трофимов О.А. Применение методов криминалистической фотографии при выявлении экономических преступлений. Вестник криминалистики. №1(85). 2022 г.; Миронова Ю.К. Методология криминалистической фотографии и видеозаписи при расследовании экономических преступлений. Москва: Юрлитинформ, 2021 г.

[2] См. об этом: Харитонов Н.Н. Особенности криминалистической фотосъемки при осмотре мест происшествий по делам о преступлениях в сфере экономики. Криминалистика и судебная экспертиза. №3(89). 2021 г.; Корнев А.М., Сергеенко С.Ю. Практическое руководство по применению криминалистической техники при расследовании экономических преступлений. Издательство РУДН, 2022 г.

Большая часть программ, предназначенных для составления фотопанорам, поставляется в комплекте с цифровыми фотоаппаратами. Однако, если это возможно, на месте происшествия ориентирующую и обзорную фотосъемку лучше выполнять методом линейной панорамной фотосъемки, чтобы избежать оптических искажений.

Характерные для круговой фотопанорамы оптические искажения могут быть устранены посредством специальных компьютерных программ. Несмотря на это, линейная панорамная фотосъемка остается наиболее рекомендуемым методом для создания панорамных фотографий.

Применительно к методике расследования преступлений в сфере экономики, панорамная съёмка имеет значение, используется и ее применение актуально при проведении осмотров участков местности, помещений, например, при расследовании хищений денежных средств, выделенных на строительство различных объектов. При помощи фотосьёмки возможно зафиксировать визуально объём выполненных работ, в том числе, если объект является большим по размеру[1].

Макросъемка — важный вид криминалистической фотографии, обеспечивающий высококачественное изображение мелких объектов и деталей. Хотя современные цифровые камеры обладают функцией макросъемки (фокусное расстояние до 1 см), специальные макрообъективы обеспечивают еще более высокое разрешение и детализацию (фокусное расстояние 1-2 см), позволяя сфокусироваться на отдельных фрагментах объекта.

Проводя взаимосвязь с предыдущим вышеописанным видом фотосъёмки, можно отметить, что указанный вид фотосъёмки может быть применен при запечатлении определенных конкретных «узлов», «механизмов», каких либо мелких деталей, что в контексте проведения осмотров объектов при

[1] См. подробней: Новиков В.Л. Осмотр места происшествия и применение специальных средств и методов в экономической криминалистике. Волгоград: ВолГУ, 2021 г.

расследовании преступлений, связанных с хищением денежных средств, выделенных на строительство, ремонт или обслуживание различных как движимых и недвижимых объектов, в том числе для фиксации качества используемых материалов, также имеет весомое значение. Указанная фотосъемка применяется как при производстве осмотра помещений/участков местности, проводимых следователем в ходе расследования, также такая фотосъёмка может быть применена экспертом в ходе осмотра, являющегося частью судебной экспертизы. Как в первом, так и во втором случае, такая фотосъёмка позволяет зафиксировать текущее состояние отдельных небольших элементов, наличие или отсутствие которых может иметь значение при расследовании преступления[1].

Помимо панорамной фотосъёмки при производстве предварительного следствия в ходе производства следственных действий активно используется измерительная фотосъемка.

Измерительная фотосъемка позволяет определять размеры и расстояния между объектами на фотографиях. Для этого рядом с объектом размещается измерительная линейка (масштаб), параллельно его длинной стороне. Использование глубинного масштаба позволяет измерять расстояния в пространстве. Камера устанавливается на штативе перпендикулярно фотографируемой плоскости.

Измерительная фотосъемка может использовать метрические инструменты, такие как рулетка с контрастной разметкой (через 3, 5 или 10 см), или размеченные веревки для секционирования места происшествия. Это позволяет определять расстояния и размеры объектов на фотографиях. Современные методы дополняются использованием навигационных данных GPS/ГЛОНАСС,

[1] См.: Васильев Г.И., Иванов Д.С. Использование фотодокументов в качестве доказательства по уголовным делам о мошенничестве в финансовой сфере. Российский следователь. №12. 2020 г.

записываемых в EXIF-данные фотоснимков (с точностью до 3 метров) при помощи специальных фотоаппаратов.

Применительно к расследованию преступлений в сфере экономики, такой метод получения информации может быть использован в различных ситуациях, например, при осмотрах местности, задачей которых является установление расстояний больших по площади территорий, что в частности, может быть использовано при расследовании преступлений, где предметом преступного посягательства выступают земельные участки.

К примеру, при расследовании мошенничеств, связанных с незаконным приобретением земельных участков, предоставляемых администрациями муниципальных образований в аренду физическим и юридическим лицам для строительства, в том числе жилищного с последующим правом выкупа участков по кадастровой стоимости участка, в большинстве ситуаций требуется зафиксировать большой по протяженности участок местности в целях фиксации отсутствия объектов капитального строительства, возведение которых на данном участке является в соответствии с Земельным кодексом РФ основанием предоставления лицам права выкупа земельных участков по кадастровой стоимости.

Также одним из способов фотосъёмки, используемом при проведении следственных действий при расследовании преступлений в сфере экономики является фотосъемка с использованием ультрафиолетового и инфракрасного излучения. Данный вид съёмки предполагает фотографирование объектов не только в видимом оптическом диапазоне, но и в инфракрасном и ультрафиолетовом излучении при помощи цифрового фотоаппарата со сменной оптикой, внешней фотовспышкой и функцией фотографирования объектов в не видимом человеческим глазом оптическом излучении. Изначально может показаться, что указанный вид фотосъёмки, предназначен больше для поиска следов при расследовании так называемых «общеуголовных» преступлений

(следов биологического происхождения по уголовным делам против половой свободы и неприкосновенности, следы мочи, синтетических красок, микроволокон хлопковых тканей и других объектов). Вместе с этим, указанная фотосъёмка может, к примеру, выявить текст на сгоревшей бумаге или бумаге, залитой чернилами, что в том числе свойственно применительно к расследованию преступлений в сфере экономики, в частности, для установления информации, содержащейся на таком документе.

Хотя ранее ультрафиолетовая и инфракрасная фотосъемка применялась лишь в сложных экспертных исследованиях из-за громоздкости оборудования, современные цифровые камеры, например, Fujifilm FinePix IS Pro UVIR, позволяют проводить такие исследования непосредственно на месте происшествия, ускоряя сбор информации. Тем не менее, это не исключает необходимости последующей экспертизы.

Тем не менее, наравне с проработкой методов производства фотографий, одним из важных вопросов является вопрос оформления результатов фотосъёмки для их приобщения к материалам уголовного дела[1].

Возможны различные варианты оформления результатов применения цифровой фотографии при производстве следственных действий.

В следственной практике в большинстве случаев при цифровой фотофиксации хода и результатов осмотра места происшествия, фотоснимки печатают уже после окончания производства следственного действия и оформления протокола следственного действия.

Также имеются случаи, при которых фототаблицу составляют на месте производства фотосъемки и предъявляют понятым. Понятые сличают

[1] См. об этом: Кириллов В.Б. Документальная фиксация доказательств в процессе расследования преступлений против собственности и порядка осуществления экономической деятельности. СПб: Юридический центр Пресс, 2020 г.; Семенов Е.П. Фотографический метод фиксирования документов при расследовании налоговых преступлений. Следователь. Федеральное агентство правовой информации. №4. 2023 г.; Федоров Б.Г. Современные технологии криминалистической фотографии в раскрытии и расследовании коррупционных преступлений. Проблемы совершенствования правоохранительной системы России. №1(27). 2022 г.

изображение на фотоснимке с объектом фиксации и удостоверяют фотографии своими подписями в фототаблице, которая изготавливается сразу же на месте проведения следственного действия. В дальнейшем фототаблица прилагается к протоколу следственного действия, но исходный носитель информации с цифровыми фотоснимками к протоколу не прилагается.

В рассмотренном варианте оформления результатов применения цифровой фотосъемки при производстве следственных действий есть несколько существенных недостатков.

Первый недостаток заключается в том, что фототаблица, составленная на месте производства фотосъемки, не содержит исходный носитель информации с цифровыми фотоснимками. Это нарушает требования статьи 166 УПК РФ, согласно которой к протоколу прилагаются фотографические негативы и снимки, киноленты, диапозитивы, фонограммы допроса, кассеты видеозаписи, носители компьютерной информации, чертежи, планы, схемы, слепки и оттиски следов, выполненные при производстве следственного действия.

Второй недостаток заключается в том, что без исходного носителя информации невозможно последующее увеличение программно-техническими средствами (не внося изменений и искажений в цифровой фотоснимок) для детального исследования зафиксированных следов.

Третий недостаток заключается в том, что без исходного носителя информации невозможно проверить версию о монтаже фотоснимков на компьютере средствами графических редакторов.

Другим способом оформления результатов фотофиксации в ходе проведения следственного действия является приобщение к протоколу следственного действия в качестве исходного носителя компьютерной информации - карты памяти цифрового фотоаппарата.

В этом случае использование карты памяти цифрового фотоаппарата как источника компьютерной информации в протоколе следственного действия имеет определенные недостатки. Карты памяти, используемые в цифровых

фотокамерах, не являются надежными носителями информации, поскольку они могут быть изменены, скопированы, перезаписаны, модифицированы или удалены. Это может потребовать дополнительных средств для подтверждения целостности и неизменности информации. В связи с этим, при сборе компьютерной информации в ходе следственных действий рекомендуется использовать более надежные носители, такие как компакт-диски, флеш-накопители или другие типы записи, которые обеспечивают надежную сохранность и неизменность информации[1].

Наряду с вышеописанными способами оформления результатов осуществления фотосъёмки, информация с карты памяти цифрового фотоаппарата зачастую копируется на одноразовый CD или DVD-диск для последующего приобщения к материалам дела[2]. Одноразовый характер оптических дисков гарантирует сохранность и неизменность данных. Однако, копирование на ПК создает уязвимость: возможность редактирования изображений на компьютере ставит под сомнение достоверность информации на диске. Процесс копирования непрозрачен и трудно контролируем. Для подтверждения подлинности данных может потребоваться заключение комплексной экспертизы.

Помимо вышеизложенных способов копирования информации, известен способ копирования фотоизображений с карты памяти цифрового фотоаппарата на одноразовый оптический диск формата CD или DVD без использования компьютера для последующего приобщения последних в качестве приложения к протоколу следственного действия. Указанный способ приобщения результатов фотографирования возможен посредством использования портативных универсальных многофункциональных рекордеров, таких как Sony DVDirect,

---

[1] См.: Павленко С.Ф. Оформление результатов фотофиксации предметов и документов при производстве судебных экспертиз по делам о преступлениях в сфере экономики. Журнал российского права. №7. 2023 г.; Петрова И.А. Формы закрепления и анализа фотографий при исследовании бухгалтерской документации. Экономическая безопасность государства. №2(46). 2021 г.

[2] См. об этом: Ильин М.Б., Терентьева Т.Р. Организация судебно-криминалистической фотографии. Закон и право, № 4, 2023.

предназначенных для копирования фотографической информации, чтобы предотвратить искажение или внесение изменений в файлы фотоизображений.

Для обеспечения целостности данных, фотографии с карты памяти фотоаппарата копируются на CD-диски без изменений. CD-R предпочтительнее DVD-R из-за меньшей плотности записи, что делает информацию более устойчивой.

Следует отметить, что в следственной практике в большинстве своем результаты фотофиксации оформляются стандартной фототаблицей на бумажном носителе, которая подписывается специалистом, проводившим фотофиксацию, либо следователем или оперативным сотрудником, которому было поручено проведение отдельных следственных действий по уголовному делу. Не смотря на то, что фактически понятые или участвующие в следственном действии лица, не заверяют своими подписями указанную фототаблицу, вопросы достоверности фотографий, приобщенных к ней, возникают не часто. Тем не менее, при возникновении таких споров, сомнения в достоверности возможно разрешить несколькими способами: как посредством допросов специалиста, оперуполномоченного или следователя (в ходе судебного следствия), так и посредством допросов понятых или иных участвующих в ходе следственного действия лиц с предъявлением последним вышеуказанных фототаблиц.

Помимо фотосъемки, одним из актуальных способов фиксации следовой картины преступления при производстве следственных действий является видеосъёмка.

Так, видеозапись при производстве следственных действий предназначена для фиксации в динамике как визуальной, так и звуковой информации, получаемой в ходе следственных действий. Видеосъёмка в процессе расследования преступлений довольно часто используется как при производстве допросов, так и при производстве проверок показаний на месте, следственных экспериментов. Применительно к процессу расследования преступлений в сфере экономики, использование видеосъёмки преимущественно осуществляется при

производстве допросов, а рассматривая аспекты проведения следственных действий с использованием видео-конференц-связи, где применение видеозаписи следственных действий является обязательным – то и при производстве очных ставок. Также видеозапись хода и результатов следственного действия может использоваться как образцы голоса лица, чей голос требуется идентифицировать в ходе предварительного следствия.

Так, к примеру, при расследовании уголовного дела по ч. 4 ст. 159 УК РФ по факту хищения бюджетных денежных средств в рамках исполнения государственного контракта, следователем проведена выемка аудиозаписи судебного заседания, содержащей условно-свободные образцы голоса подозреваемого Ш. в целях дальнейшего назначения и проведения судебной фоноскопической экспертизы[1].

Касаемо применения видеозаписи при производстве следственных действий в научной литературе существует множество рекомендаций. Во-первых, ввиду того, что на экране синхронно воспроизводится как образная, так и звуковая информация, то съемку фильма нужно проводить так, чтобы были доброкачественно зафиксированы не только изображение, но и звук[2].

Основные операторские техники включают панорамирование, наезд и отъезд. Панорамирование бывает статическим (медленный поворот камеры вокруг оси, создающий горизонтальные или вертикальные изображения) и динамическим (съемка с движущейся камеры, например, линейная панорама вдоль объекта или панорама следования за движущимся объектом). Для плавности переходов панорамы начинаются и заканчиваются статичными кадрами, с возможными остановками для акцента на важных элементах. Наезды (от общего к крупному плану) и отъезды (обратный процесс) помогают поддерживать контекст сцены.

---

[1] Из практики работы Следственной части по расследованию организованной деятельности СУ УМВД России по Калининградской области за 2023 год.

[2] См. подробней об этом: Егорова И.Н., Костылев Ф.С. Правовые основы фиксации хода и результатов следственных действий. Москва: Проспект, 2020.

Рассматривая рекомендации относительно требований к указанию сведений о применении видеофиксации при составлении протокола следственного действия, следует отметить, что согласно части 5 статьи 166 УПК РФ, протокол должен содержать информацию о видеозаписи, включая описание используемой аппаратуры, условия съемки, время начала и окончания записи, а также все паузы с указанием причин и длительности[1].

Протокол должен содержать следующую информацию: модель и тип видеокамеры; режим и уровень сжатия записи; тип, марку и емкость носителя информации; модель и тип внешнего микрофона (если использовался); условия записи; модель и тип устройства воспроизведения видеозаписи.

В случае, если копирование происходило без использования компьютера с помощью многофункционального рекордера на одноразовом оптическом диске, то этот факт необходимо отразить в протоколе следственного действия.

Для предотвращения подмены или изменений необходимо указать следующие тип диска, марка, емкость, продолжительность записи и заводской номер.

Эти данные помогут индивидуализировать диск и защитить запись от изменений. Невозможно вносить изменения в видеозапись на одноразовом диске, что исключает возможность подмены информации[2].

Выделяя отличительные в большей части положительные стороны видеозаписи как способа фиксации хода и результатов следственного действия, следует отметить, что такой «факультативный» способ фиксации доказательственной информации требует от следователя соблюдения и

---

[1] См.: Матросов Б.В. Судебная видеозапись и её значение в уголовном процессе. Новосибирск: Наука-Пресс, 2021.

[2] Подробней об этом: Холопов А.В. «Использование видеозаписи при производстве допросов на предварительном следствии», Журнал «КриминалистЪ. №1(8)», С-Пб, 2011

выполнения определенных действий, в целях соблюдения как тактических, так и процессуальных тонкостей[1].

Анализируя и обобщая комплекс таких действий, представляется возможным выработать следующий алгоритм последовательности применения следователем средств видеофиксации в ходе производства следственных действий. Данный алгоритм условно можно разделить на три этапа.

Видеофиксация следственного действия состоит из трех этапов. Первый (планирование): определение необходимости привлечения специалиста по видеозаписи; подбор и подготовка оборудования (камера, оптика, освещение и т.д.). Второй (проведение): оглашение информации о следственном действии (после включения камеры), разъяснение прав участникам; фиксация всех перерывов в записи с указанием причин. Третий (завершение): составление протокола (если не составлялся ранее), его оглашение и фиксация замечаний; просмотр записи (при возможности); упаковка носителя с записью и заверение упаковки подписями.

Во время видеосъемки следственного действия рекомендуется: 1) снять крупным планом участников при их представлении; 2) обеспечить присутствие всех участников в кадре на протяжении всего действия, особенно при допросах, очных ставках, проверках показаний на месте и следственных экспериментах[2].

В целях придания большей наглядности видеозаписи, примененной, к примеру, в ходе допроса или очной ставки, может быть сделана её стенограмма. Вместе с тем, производство таких стенограмм занимает достаточно большое количество времени и не всегда время, затраченное на производство такой стенограммы, в должной мере обеспечивает цели ее изготовления. Для изготовления стенограмм также могут применяться специальные программы-транскрайберы, обеспечивающие перевод звуковой дорожки в письменный

---

[1] См. об этом: Щукин В.В. Актуальные вопросы применения видеозаписи в современном уголовном процессе. Следователь, № 5, 2020.

[2] См.: Соколов А. Б., Горшков М. М. Видеозапись как дополнительный способ фиксации хода и результатов следственного эксперимента: организационный и содержательный аспекты // Вестник БелЮИ МВД России. 2023. №2.

вариант, а также программы, обеспечивающие синхронный перевод (в настоящее время в уголовно-процессуальной сфере применение таких методов не развито, в том числе ввиду отсутствия как ведомственного лицензируемого софт-обеспечения).

Тем не менее, учитывая, что УПК РФ не предусматривает обязательность изготовления текста фонограммы в случае применения в следственном действии средств видеофиксации, то фонограмма по результатам видеозаписи хода и результатов следственного действия может быть составлена только по инициативе следователя или лица проводящего дознание.

В частности, составление фонограммы может иметь свою значимость в случае, если допрашиваемое лицо оспаривает правильность указания в протоколе каких-либо показаний и излагает в протоколе следственного действия свои замечания. В таком случае составление стенограммы видеозаписи следственного действия может устранить указанные противоречия и придать большей наглядности и удобства, в том числе для последующего исследования указанных доказательств в ходе судебного следствия.

Таким образом, применение видеозаписи в процессе следственных действий, безусловно, является дополнительным средством, обеспечивающим объективность, иллюстративность и достоверность хода проведения следственного действия, а также его результатов.

Рассматривая различные способы фиксации следовой картины преступления в ходе производства следственных действий, следует отметить, что одним их источников получения доказательственной информации при расследовании преступлений, является сеть «Интернет».

В настоящее время уполномоченными представителями правоохранительных органов активно используется контекстный поиск в ресурсах Интернета, который позволяет собирать необходимую информацию для формирования объективного представления о предполагаемом или уже совершённом преступлении, а также для характеристики подозреваемого лица.

Эта информация дает возможность правоохранительным органам быстро реагировать на неправомерные действия в обществе и, если требуется, применять соответствующие меры для выявления, пресечения и предотвращения преступлений в соответствии с законодательством Российской Федерации[1].

Современное использование интернет-данных стало важнейшей частью работы правоохранительных органов, что связано с широким внедрением информационных технологий в повседневную жизнь. Этот процесс осуществляется в рамках анализа обстоятельств преступления и изучения личности подозреваемого. Тем не менее, получение полноценной информации о преступлении посредством компьютерного анализа не всегда возможно, поэтому даже при отсутствии данных о правонарушении в Интернете, компьютерные сведения остаются значимыми для правоохранительных органов для аналитической поддержки мероприятий, направленных на раскрытие и предотвращение преступлений.

Говоря о целесообразности фиксации и закрепления доказательственной информации, которая находится в открытом доступе в сети Интернет, важно отметить, что довольно большой пласт преступлений в сфере экономики, совершен с использованием именно указанной сети. Так, применительно к преступлениям, связанным с так называемыми «финансовыми пирамидами», для фиксации следовой картины таких преступлений, в частности установления необходимого обстоятельства, подлежащего доказыванию – обмана, требуется зафиксировать Интернет сайт, на котором размещены сведения о возможности выгодного «вложения» денежных средств под высокий процент, гораздо превышающий процентную ставку банков, и их «приумножения» (так называемые «народные кооперативы»).

При расследовании и других преступлений в сфере экономики важно зафиксировать информацию, размещенную в Интернет-сайтах. К числу таких

[1] См. подробней: Берова Д.М. Особенности использования компьютерной информации из сети «Интернет» при расследовании преступлений в Российской Федерации // Пробелы в российском законодательстве. Юридический журнал, М., 2020).

преступлений можно отнести и преступления в сфере долевого строительства (сайты с информацией о застройщике, проекте строительства, проектной документацией), также преступления, связанные с незаконной игорной деятельностью (сайты на которых размещена соответствующая информация).

Помимо вышеизложенного, фиксация открытой информации, размещенной, например, в социальных сетях позволяет установить возможные связи фигурантов преступлений между собой, их места встреч.

При этом, в целях подтверждения факта принадлежности страницы в социальной сети конкретному лицу, следует проводить дополнительные следственные действия. Например, направление запросов в организацию, обеспечивающую функционирование социальной сети, допросы родственников, знакомых, иных лиц, с предъявлением сведений о странице фигуранта в социальной сети.

Как утверждает Е.П. Ищенко, ключевая задача применения сети Интернет в расследовании уголовных дел заключается в выявлении и извлечении из сети информации, имеющей криминалистическую ценность, для последующего анализа. Рассматривая значимость сети Интернет со стороны криминалистики, можно отметить, что всё разнообразие доступных в сети Интернет данных можно условно разделить на две главные категории: а) информация, отражающая различные аспекты механизма совершения преступления и способная служить доказательствами; б) данные, которые помогают следователю или дознавателю ориентироваться в событиях, фактах и явлениях, так или иначе связанных с преступлением, которое подлежит расследованию, а также с самим процессом следствия[1].

Цели применения сети Интернет, озвученные Е.П. Ищенко, могут быть значительно детализированы. В сфере оперативно-розыскной деятельности, информационные технологии, основанные на ресурсах сети Интернет, могут служить, во-первых, источниками актуальных данных.

[1] См. об этом: Ищенко, Е.П. Виртуальный криминал: монография. – Москва: Юрлитинформ, 2011. – 208 с.; переиздание – 2013 г.

Во-вторых, каналами для быстрого взаимодействия с общественностью, а также средствами воздействия на него с целью раскрытия, расследования и предотвращения преступлений. В-третьих, данные технологии могут быть использованы для влияния на лиц, совершивших правонарушения. Например, в целях побуждения их к добровольной явке с повинной с признанием вины или к таким действиям, которые приведут к их задержанию.

Двусторонняя природа информационных процессов, происходящих в сети, способствует этому явлению. С одной стороны, сеть Интернет выступает в качестве средства массовой информации, а с другой — как инструмент коммуникации, который обеспечивает обмен осмысленными сообщениями через знаковые формы. Эта характеристика Интернета дает возможность оперативным службам вести активную информационную работу с населением для раскрытия и расследования преступлений.

В юридической литературе часто подчеркивается, что для использования информации, доступной в сети Интернет, требуется проведение множества оперативно-розыскных мероприятий для проверки этих данных и выявления лиц, совершивших правонарушения[1]. Однако на практике наблюдается высокая эффективность применяемой информации при надлежащем реагировании, что способствует профилактике и предотвращению преступлений. Следовательно, использование сети Интернет становится действенным инструментом для выявления потенциальных преступников.

При анализе практических аспектов применения компьютерной информации в расследованиях преступлений можно выделить следующие моменты:

---

[1] См. об этом: Шаров В.И. Оперативно-розыскные мероприятия в сети Интернет // Общество и право. 2018. №2 (64); Моляров Е. А., Седиев У. А. Поисковый запрос в публичной сети интернет как способ наведения справок в оперативно-розыскной деятельности // Научный компонент. 2022. №1 (13); Тимофеев С.В. Информационное обеспечение противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий // Известия ТулГУ. Экономические и юридические науки. 2021. №1.

1) Поиск доказательной информации в сети Интернет становится одной из ключевых операций; он включает контекстный поиск, который осуществляется последовательно и сопоставляется с заданными критериями. Современные методы поиска также охватывают анализ графики и звука, а не ограничиваются только текстами.

2) При фиксации доказательств, размещенных в сети Интернет, необходимо учитывать возможность их изменения и удаления. Для проведения обысков важно определить местоположение компьютеров или других устройств, использовавшихся для размещения информации. Протоколы должны фиксировать характеристики исследуемых устройств и их индивидуализирующие признаки.

Указанный выше контекстный поиск может быть процессуально оформлен протоколом осмотра предметов – в частности конкретного персонального компьютера, имеющего доступ к выходу в сеть Интернет, а также в случае производства оперативно-розыскных мероприятий – актом проведения соответствующего оперативно-розыскного мероприятия, в частности, «получение компьютерной информации».

Помимо этого, при расследовании преступлений в сфере экономики могут применяться так называемые ГИС-технологии, суть применения которых заключается в нанесении на карты мест происшествий, маршрутов передвижения, географического распределения преступлений, что может быть использовано при расследовании преступлений, связанных с незаконным приобретением права собственности на земельные участки, а также при расследовании мошенничеств в сфере строительства.

Делая вывод о проблемах правовой регламентации применения информационных технологий, предназначенных для фиксации следовой картины преступления, совершенного в сфере экономики, считаем необходимым отметить, что привлечение понятых к участию в следственных действиях, связанных с копированием информации с электронных носителей является

нецелесообразной. Необходимость в участии понятых при производстве копирования информации с электронных носителей отсутствует, поскольку при копировании информации, сведения о скопированной информации, а именно о времени, дате, устройстве, с которого была скопирована информация, отображаются в свойствах скопированного файла. При этом, указанные сведения довольно затруднительно зафиксировать в ходе следственного действия понятому в своей памяти.

Обязательность привлечения к следственным действиям, связанным с изъятием электронных носителей информации либо копированием с них электронной доказательственной информации специалиста также отсутствует. Решение об участии специалиста, как и об участии понятых должно приниматься следователем по собственной инициативе исходя из следственной ситуации.

Считаем верным исключить из ч. 2 ст. 164.1 УПК РФ требование об обязательном участии понятых и специалиста в ходе изъятия электронных носителей и копирования с них информации.

Кроме того, анализом законодательства и следственной практики выделены особенности производства криминалистической видеосъёмки, фотофиксации при расследовании различных преступлений в сфере экономики, а также подчеркнута значимость поиска доказательственной информации, находящихся в открытом доступе в сети Интернет при расследовании преступлений в сфере экономики, с учетом особенностей их правовой регламентации, что делает процесс расследования преступлений более эффективным.

Разработанные и представленные рекомендации по алгоритмизации первоначальных следственных действий при расследовании преступлений в сфере экономики, ситуационная обусловленность которых требует получения электронной доказательственной информации, направлены на комплексное и эффективное планирование следственных действий в целях своевременной

фиксации более полной следовой картины преступления и избежание утраты важных следов.

2.2. Тактические особенности проведения допросов с использованием видео-конференц-связи

Существующая потребность в проведении допросов через видео-конференц-связь возникает как из желания обеспечить дополнительную защиту для свидетелей и потерпевших, так и из-за сокращения временных и финансовых затрат при проведении следственных действий с лицами, находящимися далеко от места расследования.

В декабре 2021 года в силу вступила статья 189.1 УПК РФ, которая подразумевает проведение допросов, очных ставок и предъявлений для опознания с использованием систем видеоконференцсвязи. На сегодняшний день эти технологии постепенно внедряются в практику.

Тем не менее, хотя механизм проведения следственных действий с применением видеоконференций был официально установлен в законе еще в конце 2021 года, на практике он пока не получил должного алгоритмизированного применения со стороны следователей. Процессуальные и тактические аспекты реализации таких действий также не стали предметом глубокой научной проработки в области криминалистики и уголовного процесса, включая вопросы, касающиеся допросов.

С учетом того, что реальная практика применения данной нормы права достаточно ограничена, при возникновении следственных ситуаций, которые требуют проведения действий с участниками процесса, находящимися на значительном расстоянии от места предварительного следствия, возникают вопросы, касающиеся организации процедур и тактики таких следственных действий.

Так как допрос является наиболее распространенным следственным действием, осуществляемым с использованием видео-конференц-связи, целесообразно выделить основные проблемы, возникающие в процессе его проведения, а также обсудить его особенности и преимущества.

Изучив положения статьи 189.1 УПК РФ, можно определить порядок проведения допроса с использованием видеоконференцсвязи. Следователь, в производстве которого находится уголовное дело, выдает отдельное поручение о проведении следственных действий следователю, дознавателю или в орган дознания по месту нахождения лица, чье участие в следственном действии необходимо. После того как обеспечивается участие данного лица, допрос осуществляется с использованием видеоконференцсвязи государственных органов, проводящих предварительное расследование[1].

В процессе проведения следственного действия задействованы два следователя. Один из них находится по месту предварительного расследования, и непосредственно проводит допрос, формулируя вопросы, документируя ход и результаты следственного действия, а также составляет протокол. Второй следователь находится там, где находится участник следственного действия, чье присутствие признано необходимым - на значительном расстоянии от места предварительного расследования. Его обязанности включают организацию участия этого лица в процессе следственного действия, разъяснение ему его процессуальных прав и составление процессуального документа на основании результатов следственного действия – подписки о разъяснении прав и процедуры. В этой подписке фиксируются замечания по дополнению и уточнению протокола, составленного следователем, проводящим следственное действие, а также заявления, сделанные в ходе следственного действия[2].

В криминалистической науке существуют разные мнения о целесообразности использования дистанционных технологий для проведения допросов. Некоторые исследователи критикуют этот подход, утверждая, что одним из его основных недостатков является отсутствие физического

---

[1] См. об этом: Афанасьева С. И., Добровлянина О.В. Правовое регулирование производства следственных действий с использованием видео-конференц-связи по действующему УПК РФ // Ex jure. 2022. №4.

[2] См. подробней: Ушаков А.Ю., Кирянина И.А. О введенной в уголовно-процессуальный закон норме, позволяющей проводить отдельные следственные действия посредством дистанционных ресурсов // Вестник БелЮИ МВД России. 2023. №1.

визуального контакта между следователем и допрашиваемым. При использовании видеосвязи следователь может столкнуться с затруднениями в интерпретации эмоционального состояния свидетеля, сложности в оценке его реакции на предоставляемую информацию, а также трудности в установлении доверительной связи, что легче достигается в традиционном формате допроса[1].

Психологический контакт между следователем и допрашиваемым играет значительную роль и в большинстве случаев может существенно повлиять на результаты допроса. В этом контексте видеоконференции могут быть наиболее полезны при проведении дополнительных допросов, например, для уточнения важных деталей уголовного дела. Когда следователь уже установил первоначальный контакт с допрашиваемым в ходе первого допроса, необходимость в создании нового психологического контакта при повторном допросе через видео-конференц-связь отпадает.

В дополнение к вышеизложенному, можно подчеркнуть, что в ходе расследования преступлений в сфере экономики характерной чертой следственных действий является наличие у допрашиваемых лиц четко сформулированных позиций по делу, что часто предшествует консультациям с адвокатами или другими специалистами в области уголовного права. В таких ситуациях значимость установления психологического контакта снижается, а стремление к доверительным отношениям с следователем теряет практическую ценность по сравнению с другими категориями дел. В условиях, когда уже не так важно, как именно будет проведен допрос — в формате видеоконференции или лицом к лицу — целесообразнее использовать видеосистемы для снижения затрат и ускорения процесса расследования.

Стоит отметить, что не все допросы сопровождаются попытками противодействия следствию. В ряде случаев, в том числе и в делах о

[1] См.: Ксендзов Ю.Ю. Тактические особенности проведения допроса посредством видео-конференц-связи // Право и государство: теория и практика. 2023. №3 (219); Рамалданов Х. Х. Цифровые доказательства, полученные путем использования систем видео-конференц-связи // Актуальные проблемы российского права. 2022. №11 (144).

преступлениях в сфере экономики, допрашиваемые могут охотно предоставить полные и правдивые показания. Это могут быть как сотрудники компаний, к примеру, руководитель которой привлекается к уголовной ответственности, так и другие лица, связанные с деятельностью организаций. В таких условиях следователю не потребуется применять весь комплекс тактических приёмов, которые необходимы лишь при физическом присутствии лица в Следственном отделе. Вместе с тем, целесообразность такого подхода должна определяться следователем исходя из тактической стороны конкретной следственной ситуации.

В контексте расследования преступлений в сфере экономики также встречаются другие трудности, осложняющие процесс допроса с применением видеоконференцсвязи. Одна из таких трудностей заключается в необходимости предоставления запрашиваемым лицам, находящимся удаленно, документов, материалов и других доказательств - для формирования вопросов по ним. Частично эта проблема может быть решена в некоторых следственных ситуациях путем отправки сканированных копий необходимых бумаг, а также ранее полученных от следователя скриншотов переписок и фотографий других улик.

Тем не менее, достаточно часто допрашиваемые заинтересованы в обозрении именно оригиналов документов для подтверждения аутентичности своих подписей и других реквизитов. Кроме того, с тактической точки зрения важно представлять оригиналы документов при допросе тех, кто подписывал определенные документы, имеющие значение для дела. Это может положительно сказаться на допрашиваемом, способствуя признанию факта подписания документа и снижению его защитной позиции, что в свою очередь убедит его в наличии у следствия достаточной доказательной базы и поможет продвижению расследования.

В противоположность этому, когда допрашиваемому показывают копию документа, он может указать на её нечеткость и попытаться оспорить её подлинность (например, действительно ли его подпись стоит на оригинале или

же она была добавлена в представленной копии с помощью техники и др.). При демонстрации оригинала такие сомнения не возникают, что увеличивает вероятность того, что допрашиваемый предоставит объективные показания.

Частичное решение данной проблемы заключается в направлении оригиналов документов следователем, ведущим уголовное дело, в органы предварительного следствия или непосредственно к следователю, отвечающему за организацию участия участника следственного действия, который живет за пределами места следствия. Передача оригиналов может осуществляться с использованием специализированных видов связи (например, через ГФС, ФГУП «ГЦСС» (Спецсвязь). Также одним из способов решения проблемы может быть отправка цветных отсканированных копий по электронной почте следователю, который находится на месте участников следственного действия, с параллельной демонстрацией на веб-камеру в процессе следственных действий. Этот подход, хотя и не заменяет просмотр оригиналов документов, но может снизить у допрашиваемого сомнения в их реальности и подлинности.

Несмотря на существующие сложности в осуществлении следственных мероприятий с использованием видеоконференцсвязи, можно выделить её определенные плюсы[1].

Одним из основных преимуществ допросов с использованием видео-конференц-связи по сравнению с традиционным методом, применяемым для допроса свидетелей или обвиняемых, находящихся в других регионах страны, является возможность непосредственного формулирования вопросов во время следственных действий. В традиционном подходе следователь готовит отдельное поручение с перечнем вопросов для допрашиваемого, что требует времени и приводит к задержкам. В условиях видео-конференции следователь может мгновенно посредством постановки вопросов допрашиваемому, уточнять

[1] См. об этом: Козловский П. В., Усольцева Д. Е. Теоретико-правовые аспекты использования средств видео конференцсвязи при производстве допроса в России и за рубежом // Вестник СИБИТа. 2022. №3; Плахота К.С. Использование следователем (дознавателем) видео-конференц-связи при производстве следственных действий // Известия ТулГУ. Экономические и юридические науки. 2022. №1.

важную информацию, которая может быть не известна ему заранее. Иными словами, использование средств видео-конференц-связи по сравнению с классическим направлением поручения о допросе, позволяет следователю, в производстве которого находится уголовное дела, сразу же формулировать дополнительные вопросы на основе полученных ответов, что значительно повышает эффективность сбора информации, необходимой для расследования уголовного дела. Таким образом, видеоконференцсвязь открывает новые горизонты для оптимизации следственных процессов.

Одной из ключевых характеристик процесса проведения следственных действий с использованием видео-конференц-связи, которую мы считаем преимуществом такого подхода, является установленная УПК РФ обязательная фиксация следственных мероприятий на видео. Этот нюанс служит надежной гарантией объективности и более точного отражения хода и результатов следственного действия, наряду с составлением протокола следственного действия. В случае сомнений в достоверности данных, зафиксированных в протоколе, видеозапись может помочь разрешить возникшие неясности.

Рассматривая тактические вопросы производства следственных действий с использованием средств видео-конференц-связи, важно обратить внимание не некоторые особенности их производства[1].

Как ранее говорилось, при проведении следственных действий с использованием видео-конференц-связи обязательно применение видеозаписи. Считаем, что с тактической стороны указанное правило оказывает благотворное влияние на процесс проведения как допросов, так и очных ставок с использованием средств видео-конференц-связи. Положительной стороной производства таких следственных действий является как раз факт непрерывной фиксации всего хода следственного действия. При таких обстоятельствах, при грамотной подготовке следователя к допросу/очной ставке в части подготовки необходимых вопросов и их последовательности, можно добиться необходимых

[1] См. подробней: Ксендзов Ю.Ю. Тактические особенности проведения допроса посредством видео-конференц-связи // Право и государство: теория и практика. 2023. №3 (219).

результатов, которыми могут быть как сообщение допрашиваемым лицом, например, избравшим позицию выдвижения «защитных» «придуманных» версий, информации, интересующей следствие – правдивой. Например, по ряду вопросов. Также, положительной стороной в ряде случаев может служить и отказ от дачи показаний допрашиваемым по ряду вопросов, заданных в необходимый момент, что также может подтверждать причастность лица к совершенному преступлению. В любом случае, положительная сторона производства таких следственных действий – факт того, что весь процесс зафиксирован на видео, в том числе и все ответы допрашиваемого лица. При таких обстоятельствах стороне защиты намного труднее будет оспорить факт получения следствием такого доказательства, в сравнении с протоколом следственного действия, где сторона защиты может сослаться на неточность изложения следователем отдельных ответов и реплик в протоколе следственного действия.

В любом случае, при производстве следственного действия, допрашиваемые лица должны сидеть непосредственно перед видеокамерами в целях того, чтобы на видеозаписи, которая в последствие будет приложена к протоколу следственного действия, находились именно допрашиваемые лица, а не кто-либо другой. Желательно также при наличии возможности, осуществить видеосъёмку таким образом, чтобы в кадр попал и защитник подозреваемого (обвиняемого) или адвокат свидетеля, в случае если он участвует в деле. Это поможет в дальнейшем опровергнуть данные допрашиваемыми лицами показания, не отвечающие действительности. Касаемо участия в следственном действии защитников и адвокатов, то обязательным требованием является контроль за их процессуальным поведением в ходе его проведения.

В ходе проведения следственного действия следователю в любом случае необходимо исключить воспроизведение адвокатом или защитником допрашиваемого лица ответов на задаваемые следователем вопросы, поскольку согласно ч. 2 ст. 53 УПК РФ он вправе только давать подзащитному в присутствии следователя краткие консультации. Следователь обязан сделать

замечание участвующему в деле защитнику или адвокату, а также занести факт допущенных им нарушений в протокол следственного действия.

В любом случае, видеозапись в таких случаях будет нести сдерживающий фактор для защитников, практикующих вышеуказанные злоупотребления своими процессуальными правами. Так, на ней будут непосредственно зафиксированы указанные нарушения, а видеозапись будет исследоваться в дальнейшем в ходе судебного следствия, а также в установленном порядке, ее копия может быть предоставлена вместе с представлением в соответствующую адвокатскую палату субъекта РФ в качестве обоснования нарушений адвоката, допущенных в ходе следственного действия, что может нести для адвоката негативные последствия в части привлечения к дисциплинарной ответственности.

Таким образом, использование дистанционных технологий для допросов представляет собой современный правовой инструмент, способствующий оптимизации расследования преступлений, а также облегчающий организацию допросов с участниками процесса, находящимися далеко от места совершения преступления.

Так, для проведения вербальных следственных действий посредством использования видео-конференц-связи по причине невозможности явки лица, проживающего на значительном отдалении от органа предварительного следствия, в следственный орган по месту его жительства предлагается их проведение с использованием электронно-цифровой подписи и функций приложения «Госключ».

Помимо этого, при производстве следственного действия с использованием видео-конференц-связи, необходимо следовать представленным тактическим рекомендациям: допрашиваемые лица должны сидеть непосредственно перед видеокамерами; видеосъёмку осуществлять таким образом, чтобы в кадр попал защитник подозреваемого (обвиняемого) или адвокат свидетеля; необходимо осуществлять контроль за процессуальным поведением участвующих в следственном действии защитников и адвокатов, в целях недопущения

формулировки ими ответов за допрашиваемых лиц и иных злоупотреблений с его стороны.

2.3 Проблемы изъятия электронных носителей информации по преступлениям в сфере экономики

На сегодняшний день подавляющая часть организаций активно использует электронный документооборот, а финансовые расчеты между ними осуществляются при помощи электронных платежных систем в безналичной форме. Кроме того, государственные контракты и контракты крупных коммерческих клиентов разыгрываются и оформляются на электронных площадках с возможностью дистанционного подписания с использованием электронно-цифровых подписей. Аукционы и торги по реализации имущества в процессе банкротства также проходят на специализированных электронных торговых платформах.

Для получения значительного объёма доказательной информации, подтверждающей умысел и объективную сторону преступления, можно анализировать файлы, хранящиеся на электронных носителях, включая финансовую и бухгалтерскую документацию, контракты и личные записи. Также полезным является изучение электронной переписки между лицами, представляющими интерес для следствия, или запросы к банкам о движении денежных средств, истории соединений между устройствами и данные по IP-адресам у провайдеров.

Современные методы получения электронной информации в уголовных делах варьируются от изъятия носителей в ходе следственных действий до альтернативного доступа к сведениям от третьих лиц, таких как провайдеры связи. Тем не менее, значительный прогресс в области технологий вносит свои сложности в процесс сбора электронной доказательной информации, на что обращают внимание ученые-криминалисты[1].

[1] См. подробнее: Васюков В.Ф. Изъятие электронных носителей информации при производстве следственных действий: новеллы законодательства и проблемы правоприменения // Вестник Томского государственного университета. Право. 2020. № 37. С. 32–39; Россинская Е.Р., Сааков Т.А. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров / Криминалистика: вчера, сегодня, завтра. Иркутск, 2020.

Одним из наиболее эффективных методов получения электронной доказательной информации является изъятие электронных носителей и копирование с них данных. Эти действия могут выполняться в ходе следственных мероприятий, таких как обыск, выемка и осмотр места происшествия, среди прочих. При этом уголовно-процессуальный кодекс требует, чтобы изъятие и копирование информации проводились с соблюдением норм статьи 164.1 УПК РФ, которая касается «Особенностей изъятия электронных носителей информации и копирования данных при проведении следственных действий». Как отмечает П.О. Панфилов, одной из задач введения данной статьи является обеспечение дополнительных гарантий защиты предпринимателей от необоснованного уголовного преследования[1].

Статья 164.1 УПК РФ создавалась, в том числе, и для предотвращения неоправданного применения мер, которые могут привести к приостановлению законной деятельности организаций или индивидуальных предпринимателей в процессе изъятия электронных носителей. В ней определены конкретные ситуации, при которых возможно изъятие, включая случаи назначения судебной экспертизы, изъятие на основе судебного акта и ситуации, когда информация на носителе может использоваться для новых преступлений или подлежит риску утраты.

В части 3 статьи 164.1 УПК РФ, предложен альтернативный способ получения доказательной информации с электронных носителей – это их копирование. В процессе осуществления данного действия к протоколу следственного мероприятия прикрепляются те электронные устройства, на которые была перенесена информация, извлеченная с других носителей в ходе расследования.

Анализируя положения статьи 164.1 УПК РФ, можно сделать вывод о том, что приоритет в сборе доказательств с электронных носителей предоставляется

[1] См. об этом: Панфилов П.О. Очередное обострение конкуренции конституционных ценностей при расследовании преступлений в сфере экономической и предпринимательской деятельности // Вестник Московского университета МВД России. - 2020. - № 1. - С. 107-113.

именно копированию данных на другие устройства, такие как оптические диски или флеш-накопители[1]. Это обусловлено тем, что такой метод извлечения информации не наносит вреда законной предпринимательской деятельности как юридических лиц, так и индивидуальных предпринимателей.

При получении доказательственной информации посредством копирования информации, содержащейся на электронных носителях информации, сотрудники правоохранительных органов не ограничивают права граждан на использование их электронных носителей, поскольку после извлечения необходимых данных, сами носители остаются у их владельцев. У органов правопорядка информация хранится на других устройствах, куда копируется информация в ходе следственных мероприятий с личных электронных носителей информации их владельцев.

Тем не менее, на практике возникают проблемы, даже при наличии четкой регламентации процесса получения доказательств с электронных носителей. Уголовно-процессуальный кодекс в статье 164.1, определяет конкретные условия, при которых возможен процесс изъятия электронных носителей при расследовании преступлений в сфере экономики: если они использовались для новых преступлений, лицо не имеет полномочий на их хранение, если изъятие производится на основании судебного решения, назначена судебная экспертиза, либо копирование информации может привести к ее утрате или изменению. В случаях, когда вышеперечисленных оснований нет, то изъятие носителей не разрешается.

Тем не менее, как уже упоминалось, в ситуациях, когда изъятие электронных носителей невозможно, доказательства могут быть собраны путем

[1] См. подробней: Мещеряков В.А. Копирование информации с компьютерных носителей при производстве следственных действий / В. А. Мещеряков, О.Ю. Цурлуй // Цифровой след как объект судебной экспертизы : Материалы Международной научно-практической конференции, Москва, 17 января 2020 года. – Москва: РГ-Пресс, 2021. – С. 128-132.

копирования данных с устройств их владельцев, что соответствует части 3 статьи 164.1 УПК РФ.

Однако процесс копирования определенных видов электронной информации, таких как переписка в мессенджерах или посредством электронной почты, не всегда может быть выполнен моментально во время конкретного следственного действия. Это связано с тем, что такая переписка в ряде случаев не хранится на самом устройстве, а может быть и вовсе удалена. Экспортировать чаты можно только через электронные каналы связи, а некоторые мессенджеры вообще не предоставляют возможности для экспорта переписки. Кроме того, может возникнуть сопротивление со стороны лица, у которого проводятся обыски. Например, если владелец электронного устройства отказывается предоставить пароли и логины для доступа к сервисам электронной почты.

Несмотря на существующие обстоятельства, потребность в получении указанной доказательной информации остается актуальной. В большинстве случаев целесообразнее изъять электронный носитель данных, нежели просто скопировать определённые важные файлы, так как тщательное исследование самого носителя (его осмотр или проведение судебно-технической экспертизы) может выявить дополнительные важные для доказывания аспекты[1]. Кроме этого, исследование носителя в условиях экспертого учреждения с подключением к стендовым компьютерам со специальными программами позволит извлечь удаленные с электронного носителя информации файлы, что невозможно сделать в процессе проведения следственного действия, проводимого за его пределами, например обыска по месту жительства фигуранта или по месту работы.

Для решения этой проблемы следует рассмотреть возможность законодательного расширения оснований для изъятия электронных носителей информации.

---

[1] См.: Васюков В.Ф., Булыжкин А.В. Изъятие электронных носителей информации при расследовании преступлений: нерешенные проблемы правового регулирования и правоприменения // Российский следователь. 2016. № 6. С. 3 - 8.

В частности, в ч. 1 ст. 164.1 УПК РФ необходимо включить новое основание, позволяющее изымать такие носители, если копирование данных невозможно по техническим причинам при наличии соответствующего заявления специалиста, участвующего в следственном действии.

Вместе с тем чтобы избежать неправомерного применения мер, которые могут воспрепятствовать обеспечению законных прав и интересов граждан, а также законной деятельности организаций и предпринимателей, целесообразно установить сроки для осмотра таких носителей и их признания вещественными доказательствами, а также сроки для назначения экспертизы (в случае, когда требуется ее назначение и проведение), по аналогии с общим сроком осмотра электронных носителей информации при расследовании преступлений экономической направленности, закрепленном в ч. 2 ст. 81.1 УПК РФ (10 суток, который может быть единожды продлен по мотивированному ходатайству до 30 суток. При этом в случае назначения экспертизы, срок вынесения постановления о признании вещественным доказательством при наличии оснований должен составлять также 3 суток).

При этом владельцам электронных носителей должно быть гарантировано право на разумный срок для копирования данных, необходимых для законной деятельности.

Таким образом, по результатам анализа проблем изъятия и осмотра электронных носителей информации, считаем необходимым дополнить статью ч. 1 ст. 164.1 УПК РФ, пунктом 4, в который включить новое основание, позволяющее изымать такие носители: «если копирование данных невозможно по техническим причинам при наличии соответствующего заявления специалиста, участвующего в следственном действии».

В ходе расследования преступлений в сфере экономики крайне важным представляется проведение тщательного и всестороннего осмотра изъятых электронных носителей информации, изъятие которых осуществляется в большинстве своем при первоначальных следственных действиях. В ходе

тщательного осмотра электронных носителей информации, возможно почерпнуть довольно большой объём и массив доказательственной информации при расследовании преступлений данной категории.

Так, к примеру, при расследовании мошенничеств, орудием совершения которых являлись поддельные (фиктивные) документы, то обнаружение их на персональном компьютере (ноутбуке, мобильном телефоне), может подтвердить причастность указанного лица к совершению указанных преступлений. Изучение переписки, содержащейся в сообщениях, сохраненных в памяти мобильных телефонов, может доказать факт совершения преступления в соучастии. При расследовании преступлений о незаконной банковской деятельности, довольно весомым доказательством будет являться нахождение на персональном компьютере «бухгалтера» документации по аффилированным юридическим лицам, индивидуальным предпринимателям, через которые осуществляется вывод денежных средств (обналичивание)[1]. По уголовным делам о неправомерном обороте средств платежа важно установить наличие на электронных носителях фигурантов банковских приложений, посредством которых осуществляется доступ к расчетным счетам открытых на подставных лиц[2]. По делам о незаконной игорной деятельности, к примеру, необходимым обстоятельством, подлежащим установлению, будет являться нахождение на изъятых устройствах (оборудовании) программ для доступа к сервисам азартных игр, информация о подключении к конкретным серверам, посредством которых осуществляется игорная деятельность и другие.

В процессе проведения данного следственного действия важно не только сосредоточиться на выявлении значимой для уголовного дела информации, но и минимизировать возможность ее утраты.

---

[1] См. об этом: Бандорина И.В. Документирование преступлений, ответственность за которые предусмотрена статьей 172 УК РФ «Незаконная банковская деятельность» // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2015.

[2] См. подробней: Карпов Н.О. Криминалистические особенности осмотра электронных носителей информации в ходе расследования неправомерного оборота средств платежей // Вестник Казанского юридического института МВД России. 2019. Т. 10, J№ 3. С. 391-395. DOI: 10.24420/KUI.2019.81.52.021

При подготовке к следственному действию рекомендуется выполнить следующие шаги:

1. Пригласить специалиста в области информационных технологий для участия в следственном действии[1]. Это может быть как эксперт из криминалистического подразделения с соответствующей квалификацией, так и специалист из другой организации, обладающий нужными навыками. Его участие критически важно, поскольку он способен не только обнаружить скрытые данные на носителе, но и предотвратить уничтожение необходимых файлов. Некоторые специалисты могут восстановить ранее удаленные данные, используя специальное программное обеспечение.

2. Определить место, где будет проводиться следственное действие. Обычно осмотр изъятых электронных носителей осуществляется в кабинете следователя, но при необходимости наличия дополнительного оборудования следует обсудить возможность проведения процедуры в экспертном учреждении[2].

3. Подготовить нужные технические средства и устройства. Необходимо заранее обсудить со специалистом, какие технические средства могут понадобиться, включая дополнительные устройства, которых у него может не быть на руках.

Особенности проведения осмотра в значительной степени зависят от разновидности электронного устройства, которое подлежит исследованию. Эти устройства могут быть как съемными, например, флэш-накопители и компакт-диски, так и встроенными. Большинство электронных носителей информации,

---

[1] См. об этом: Лубяная, Н. И. Привлечение специалиста к осуществлению осмотра, изъятия электронных носителей и копирования с них информации: проблемы теории и практики / Н. И. Лубяная // Следственная деятельность: проблемы, их решение, перспективы развития : Материалы V Всероссийской молодёжной научно-практической конференции, Москва, 03 декабря 2021 года. – Москва: Московская академия Следственного комитета Российской Федерации, 2022. – С. 230-264. – EDN BRFPUJ.

[2] См.: Маханек, А.Б. Проблемы обеспечения прав участников уголовного судопроизводства при осмотре электронных носителей информации / А. Б. Маханек // Закон и правопорядок в Третьем тысячелетии: IX Балтийский юридический форум, материалы международной научно-практической конференции, Калининград, 12 декабря 2020 года. – Калининград: Калининградский филиал Санкт-Петербургского университета МВД России, 2021. – С. 31-33. – EDN BQWFQS.

которые имеют важное значение в расследовании вышеуказанных преступлений, конструктивно включены в компьютерные системы. Это включает в себя: встроенную память настольных и портативных компьютеров, а также мобильных устройств и других подобных гаджетов[1].

При исследовании подобных устройств необходимо учитывать ряд особенностей, которые могут оказать влияние на процесс их осмотра:

1) Устройства оснащены оперативной (энергозависимой) памятью, которая теряет данные при отключении питания. Обычно в этой памяти хранятся сведения о приложениях, работающих в данный момент, и о действиях, проведенных в этих приложениях. При проверке подобных устройств со встроенными источниками питания (например, ноутбуки или планшеты) важно учитывать риск, что оборудование с момента его изъятия не было выключено. В таких случаях, прежде всего, следует проанализировать открытые приложения, и только после этого можно безопасно отключить устройство, а затем извлечь модули памяти и провести другие необходимые операции. В случае, если осмотр электронных носителей информации проводится с участием специалиста, в том числе являющимся сотрудником экспертно-криминалистического подразделения МВД России, то в ходе осмотра им может быть использован специализированный программный комплекс для получения и при необходимости оперативного извлечения из осматриваемого носителя необходимой информации, такой, например, как ПО «Мобильный криминалист»;

2) На многих гаджетах, особенно на смартфонах и планшетах, при одном нажатии кнопки «выключение» система переходит в режим гибернации, который также называют режимом сна. В этом состоянии оперативная память продолжает работать, что даёт возможность проверить открытые приложения. Однако следует учитывать, что в большинстве случаев устройство может оставаться в этом

[1] См. подробней: Мещеряков В.А., Цурлуй О.Ю. Криминалистические особенности получения компьютерной информации с цифровых носителей при производстве отдельных следственных действий // Эксперт-криминалист. 2020. № 2. С. 15–17

режиме, используя аккумулятор, в течение нескольких дней[1]. Именно поэтому важно приступить к осмотру таких устройств как можно скорее после их изъятия;

3) На современных гаджетах, в основном работающих на Android и iOS, предусмотрена функция удаленной блокировки, позволяющая владельцу заблокировать устройство. Как только блокировка активирована, доступ к устройству прекращается при его первом соединении с Интернетом. Кроме того, на современных гаджетах, в основном мобильных устройствах, существует функция возможности удаленного доступа к устройству посредством сети Интернет. Например, посредством удаленного доступа к устройству можно как стереть, добавить, так и редактировать содержащуюся на нем информацию. Яркий пример тому система icloud на устройствах, функционирующих на операционной системе iOS. Такие действия могут неблагоприятно сказаться на процессе доказывания, в случае, если такое мобильное устройство изъято без учета особенностей таких устройств.

Чтобы избежать таких последствий, перед началом проверки устройства, рекомендуется удалить сим-карту (если она есть) и переключить устройство в режим «в полете», который отключает все беспроводные соединения. Кроме того, необходимо вручную отключить «Wi-Fi», «Bluetooth» и мобильные данные.

Рассматривая вопросы сохранения наиболее полной электронной следовой картины преступления на изымаемом носителе информации, следует акцентировать внимание на некоторые нюансы, которые могут возникнуть при проведении следственных действий, связанных с изъятием электронных носителей информации. При их проведении, казалось бы, все основные криминалистические требования и рекомендации по изъятию могут быть

[1] См.: Старичков М.В. Тактика осмотра и выемки носителей компьютерной информации // Вестник Восточно-Сибирского института Министерства внутренних дел России. 2012. № 2(61).

соблюдены, вместе с тем результат следственного действия может быть отрицательным[1].

Анализируя следственную практику, следует заострить внимание на особенностях изъятия и последующего осмотра или исследования мобильных устройств (смартфонов), выпуск которых производился (производится) преимущественно с 2019-2020 годов. Это как устройства на операционных системах iOS, так и Android. Одной из особенностей указанных устройств является наличие возможности подключения так называемой e-sim, которая в отличие от обычной сим-карты является не съёмной, как мы обычно привыкли ее представлять, а встроенной в виде чипа в само устройство (смартфон).

E-SIM расшифровывается как встроенная SIM-карта и представляет собой чип, который устанавливается непосредственно на материнскую плату смартфона. В отличие от традиционных SIM-карт, он интегрирован в устройство уже на этапе его производства. Его невозможно извлечь, выбросить, установить в другое устройство или заменить на новую карту. Чаще всего e-SIM используется в современных смартфонах, особенно в флагманских моделях.

По умолчанию eSIM не имеет присвоенного номера телефона и не связана с конкретным оператором связи. Это означает, что в целом, при эксплуатации смартфона, в котором предусмотрено наличие eSIM, можно не активировать цифровую SIM-карту, а пользоваться только встроенной. Кроме этого, на многих моделях устройств есть возможность выбора на eSIM одного или несколько операторов связи и активировать под ними номера телефонов.

При таких обстоятельствах – извлечь указанную сим-карту привычным способом ее извлечения из слота, не представляется возможным. Извлечение самого чипа возможно только при механическом вскрытии устройства и

---

[1] См.: Самолаева, Е. Ю. Некоторые проблемы практики при изъятии и осмотре электронных носителей информации / Е. Ю. Самолаева // Развитие современной науки и технологий в условиях трансформационных процессов : Сборник материалов IX Международной научно-практической конференции, Москва, 22 февраля 2023 года. – Санкт-Петербург: Печатный цех, 2023. – С. 426-430.

последующем его отделении (выпаивании). При этом, не гарантирована дальнейшая полноценная работоспособность устройства.

Изъятие и последующий осмотр устройств с такими функциями имеет ряд особенностей. Например, возвращаясь к вопросу наличия на современных «гаджетах» удаленного доступа к данным мобильного устройства с иного устройства, следует отметить, что при включении мобильного телефона, в котором установлена e-sim, мобильный телефон сразу же подключится к сети Интернет (в случае, если не включен режим «в самолете» и не выключена функция «передачи данных»). Таким образом, при включении мобильного телефона, в случае, если посредством удаленного доступа лицом были приняты меры по удалению данных с устройства, они могут автоматически стереться с него. При этом, на первый взгляд, лицо, проводящее осмотр, при не знании данных возможностей, может полагать, что стандартная сим-карта извлечена из устройства, а, следовательно, мобильный телефон, при его включении, подключиться к сети Интернет не сможет. Тем не менее, как было указано ранее, такие возможности в настоящее время имеются и знание особенностей анатомии современных устройств, может предотвратить утрату значимых электронных доказательств[1].

Таким образом, следует выделить ряд рекомендаций, направленных на противодействие возможной утраты доказательственной информации при осмотре и анализе мобильных устройств, на которых может иметься e-sim:

1) Во всех случаях, при изъятии электронных носителей информации (мобильных телефонов, планшетов и иных), при наличии технической возможности, отключать функции «передачи данных», ставить режим «в самолете»; извлекать стандартную сим-карту из слота изымаемого устройства;

2) При невозможности отключить функцию «передачи данных», а также при невозможности установить режим «в самолете», незамедлительно выключать

[1] См.: Ким А.В. Отдельные вопросы проведения осмотра и экспертизы электронных носителей информации // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2019. N 5 (71). С. 151-156.

мобильный телефон. В таких случаях при включении мобильного телефона создается опасность удаления (вышеописанным способом) криминалистически значимой информации, которая может в нем содержаться. Однако необходимость во включении устройства может потребоваться при дальнейшем его осмотре или исследовании. Так, например, в ходе расследования преступления может быть установлен пароль от устройства – как посредством следственных действий, так и посредством оперативно-розыскных мероприятий.

В таких случаях необходимо создать такую обстановку, при которых в момент включения мобильного телефона и последующей его разблокировки не произошло удаления или искажения данных. В таких случаях следует привлекать к участию в следственном действии специалиста, который, в частности, обладает специальными познаниями в области радиотехники. Представляется, что в момент включения мобильного телефона специалист-радиотехник должен применить имеющиеся у него специальные устройства, предназначенные для подавления связи (подавители связи, в простонародии – «глушилки»). Указанные устройства функционируют по следующему принципу: они генерируют и рассекают так называемый «белый шум» — электромагнитные волны в заданном частотном диапазоне, не содержащие никакой информации — создавая тем самым помехи. Это похоже на то, как громкий шум от проезжающих автомобилей или работающих на фабрике механизмов затрудняет общение между двумя людьми. Информация нулевая, и при высоком уровне шума диалог не состоится.

При таких обстоятельствах риск возможной утраты содержащейся на устройстве криминалистически важной информации сводится к нулю.

Таким образом, предложенный алгоритм решает следующую задачу – помогает включить устройство, в котором может находиться e-sim, без риска возможного уничтожения данных разблокировать его при наличии пароля, а при его отсутствии посредством применения аппаратно-программных комплексов экспертных подразделений и далее проводить исследование.

Также возможен вариант производства указанной последовательности действий в целях подготовки устройства для последующей экспертизы или детального осмотра (исследования). В таком случае приглашается специалист, который помогает посредством активации подавителей связи «заглушить» устройство, а после при его включения и разблокировки активируется режим «в самолете», который при дальнейших осмотрах и исследованиях защищает от риска утраты информации. Разумеется, после установки режима «в самолете» (режима «полета») привлечение специалиста-радиотехника для включения аппарата уже не будет необходимым, следственные действия возможно будет проводить в его отсутствие.

Таким образом, знание особенностей вышеуказанных современных мобильных устройств, в том числе особенностей функционирования e-sim, позволяет своевременно должным образом осуществить подготовку и проведение следственных действий, направленных на установление и закрепление электронной доказательственной информации, а также предотвратить риск ее утраты или уничтожения.

В науке криминалистики разработаны различные алгоритмы производства осмотра электронных носителей информации[1]. Проводя их анализ в совокупности, представляется возможным сформировать основные этапы (позиции), которые необходимо осуществить при производстве указанных следственных действий:

1) Определить технические характеристики устройства, а также его форму, тип и предназначение[2];

2) Проанализировать внешний вид устройства с целью выявления надписей, физических повреждений, уникальных черт и других особенностей;

---

[1] См. об этом: Шушеначев А.В. Правовое регулирование сбора цифровой информации с целью ее представления как доказательства в расследовании преступлений // Юридическая наука. 2023. №1; Гончар В.В., Галиев Д.В. Особенности осмотра и изъятия электронных носителей информации с учётом требований ст. 164. 1 УПК РФ // Вестник Московского университета МВД России. 2020. №2.

[2] См.: Федулова А.Е. Электронные носители информации в уголовном судопроизводстве // Юридическая наука и правоохранительная практика. 2022. №2 (60).

3) Оценить техническое состояние носителя информации (размеры, уникальные признаки и так далее);

4) Выяснить наличие разъемов у устройства, а также их количество и состояние для подключения к считывающему оборудованию;

5) Проверить, существуют ли признаки защиты носителей информации, а также выяснить имеются ли риски утраты или уничтожения криминалистически важной информации при включении устройства или при его подключении к стендовому компьютеру (считывающему оборудованию);

6) При возникновении риска утраты или уничтожения криминалистически значимой информации принять своевременные меры по недопущению их утраты. Например, привлечь соответствующих специалистов для оказания помощи в разблокировке устройства без потери искомых данных, а также их извлечения;

7) С использованием специального программного обеспечения провести анализ данных на носителе на наличие вредоносных программных средств;

8) Выполнить поиск зашифрованных, скрытых и ранее удаленных файлов.

С учетом широкой популярности облачных хранилищ, при осмотре обязательно стоит проверить наличие доступа к ним на рассматриваемом устройстве[1]. Облачные хранилища — это разнообразные серверы, которые предоставляют пользователям определенное количество пространства для хранения их данных, такие как «iCloud», «Яндекс.Диск», «Google Drive», «OneDrive», «Облако Mail.Ru». Обеспечение доступа к этим хранилищам возможно исключительно через Интернет. В подобных ситуациях целесообразно зафиксировать содержимое облачных хранилищ — фотографированием, видеосъемкой или копированием данных — пока устройство подключено к интернету во время изъятия. После этого рекомендуется перевести устройство в режим полёта.

[1] См. об этом: Кузьмин М.Д. Проблемы расследований преступлений, совершенных с использованием облачных хранилищ в сети интернет // Полицейская деятельность. 2020. №1; Нестеров А.Д., Баркалов Ю.М. Получение информации из облачных хранилищ при расследовании инцидентов в сфере информационной безопасности // Advances in Law Studies. 2015. Т. 3. № 2. С. 59-62.

При осмотре электронных носителей информации при расследовании преступлений в сфере экономики, в частности, мошенничеств в сфере экономической деятельности, а также иных преступлений, связанных как с незаконной банковской деятельностью, незаконным получением кредитов и иных, следует отметить, что зачастую объектом поиска служат электронные документы (проекты документов)[1]. Они могут представлять собой документы, созданные от имени аффилированных юридических лиц; документы, созданные от имени организаций, зарегистрированных на подставных лиц (так называемых «номинальных директоров»); проекты документов, содержащих недостоверные сведения (фиктивные договоры, иные документы, содержащие заведомо ложные сведения о понесенных организацией расходов на приобретение товаров, выполнение работ, уплате обязательных платежей и другие), которые зачастую используются для дальнейшего предоставления в уполномоченные государственные органы в целях хищения денежных средств путём обмана (посредством получений субсидий, компенсаций, оплаты в рамках контрактных обязательств и др.).

При осмотре электронных носителей в таких случаях важно обращать внимание и фиксировать в тексте протокола осмотра электронного носителя информации следующие атрибуты:

1) Время создания электронного документа;

2) Дату и время внесённых в документ правок, а также их количество.

3) Содержание изменений, что можно выяснить, сравнивая исследуемый документ с его ранними версиями, методом восстановления удалённых данных.

4) Наличие предыдущих версий документа, которые могут находиться в архивных каталогах или в "корзине".

5) Наличие резервных копий документа.

6) Сопоставление текста электронного документа с существующими печатными версиями и образцами.

[1] См.: Галяутдинов Р. Р., Коваленко В. А. Тактика осмотра электронных документов // Международный журнал гуманитарных и естественных наук. 2022. №10-3.

Кроме того, во время производства осмотра электронных носителей данных крайне важно производить последовательную и детальную фотосъемку экрана устройства, на котором отображается информация, имеющая доказательственное отношение к уголовному делу.

2.4. Проблема получения электронной информации о переписках у операторов и провайдеров

Рассматривая пути получения электронной доказательственной информации при расследовании преступлений, не является правильным ограничиваться только на вопросах изъятия электронных носителей информации, копирования с них доказательственной информации, а также на вопросах осмотра изъятых электронных носителей информации и носителей, на которые произведено копирование доказательственной информации. Зачастую при расследовании преступлений в сфере экономики, электронные носители информации, в том числе содержащие необходимые электронные сообщения, переписки, не представляется возможным обнаружить в ходе следственных действий (что обычно связано с противодействием расследованию в форме намеренного сокрытия или уничтожения указанных носителей информации), а обнаруженные электронные носители информации, которыми могут являться как мобильные телефоны (смартфоны), так и ноутбуки, персональные компьютеры, планшетные компьютеры, могут иметь достаточно сильные средства защиты, которые при наличии пароля, не представляется возможным взломать, в том числе и при проведении специальных исследований и экспертиз. Такими электронными носителями информации в частности являются мобильные телефоны, ноутбуки, функционирующие на системе IOS (всеми известные Apple Iphone, Apple MacBook и иные).

*Так, в ходе проведенной компьютерно-технической судебной экспертизы по уголовному делу № 122012700130000**, расследуемого Следственной частью Следственного управления УМВД России по Калининградской области по ч. 2. ст. 196 УК РФ, эксперту не представилось возможным ответить на поставленные следователем вопросы относительно наличия в содержимом мобильного телефона Apple Iphone XS, принадлежащем подозреваемому, искомых данных (файлов: текстовых и медиафайлов; сведений об имеющихся*

текстовых и иных сообщениях), по причине того, что следователем эксперту не был предоставлен пароль от мобильного телефона. При этом, владелец мобильного телефона в ходе его изъятия при производстве обыска отказался сообщить пароль от указанного устройства[1].

Указанные факторы обуславливают необходимость в поиске иных средств и методов получения указанной доказательственной информации посредством альтернативных источников[2].

В первую очередь, речь идет о возможностях получения СМС-сообщений, переписки посредством электронной почты, переписки в социальных сетях и мессенджерах.

Во вторую очередь, речь может идти, в том числе и о получении информации и о файлах (текстовых, аудио, видео, фото), которые хранятся на устройствах интересующих следствие лиц. О получении указанной информации речь может идти в тех случаях, при которых указанная информация хранится в так называемых «облачных» хранилищах речь о которых в том числе мы вели раньше.

Таким альтернативным методом сбора электронной доказательной информации при расследовании преступлений являются такие следственные действия, как «выемка электронных сообщений в организациях, осуществляющих передачу данных по сетям связи» и «получение данных о соединениях между абонентами и их устройствами». Также направляются запросы к интернет-провайдерам и сетевым провайдерам. Указанные мероприятия предполагают обращение к провайдерам для получения доказательственной информации, которая хранится на их серверах.

---

[1] Из практики работы Следственной части по расследованию организованной преступной деятельности УМВД России по Калининградской области за 2023 г.

[2] См. об этом: Волчецкая Т.С. Влияние цифровых технологий на современное развитие криминалистической науки // Современные технологии и подходы в юридической науке и образовании. Сборник материалов международного научно-практического форума. Калининград, 2021. С. 148-155.

На сегодняшний день практика получения подобной информации существует. Российские интернет и сетевые провайдеры, получая следственные запросы, предоставляют необходимые для расследования данные, такие как информация о местонахождении устройств, подключенных к Интернету по IP-адресам[1].

Кроме того, в российских организациях, обеспечивающих передачу сообщений по сетям электросвязи, по решению суда может быть произведена выемка сообщений электронной почты, переписки в социальных сетях. Законодательно, такой механизм предусмотрен в ч. 7 ст. 185 УПК РФ и введен в действие еще в 2016 году. Фактически, указанный механизм сводится к получению судебного решения в установленном ст. 165 УПК РФ порядке и в дальнейшей выемке на его основании в организации, обеспечивающей передачу информации по сетям электросвязи (компании почтового сервиса, социальной сети). При этом, в ходатайстве перед судом о производстве выемки очень важно указывать о необходимости выемки как имеющихся на электронном почтовом ящике электронных сообщений, так и о необходимости выемки электронных почтовых сообщений, удаленных с почтового ящика.

*Так, в ходе расследования уголовного дела № 119012700130001**, расследуемого Следственной частью Следственного управления УМВД России по Калининградской области по обвинению А. и Ш. в совершении преступления, предусмотренного ч. 4 ст. 159 УК РФ, следователем на основании судебного решения произведена выемка в ООО «ВК» сведений о входящих и исходящих сообщениях электронных почтовых ящиков ***@mail.ru, ***@bk.ru. В дальнейшем, в ходе осмотра содержимого электронных сообщений удалось установить факт пересылки между обвиняемыми проектов фиктивных договоров, заключенных в дальнейшем в рамках государственного контракта и отчетных документов по ним, которые в дальнейшем представились в УФК по*

[1] См.: Архипова Н.А. Тактика осмотра и выемки электронных сообщений, передаваемых по сетям электросвязи // Закон и право. 2018. №6.

*Калининградской области в целях оплаты за фактически не поставленное в адрес ФГУП «***» оборудование*[1].

При этом, как было сказано ранее, следует выходить с указанным ходатайством как можно скорее, поскольку указанная удаленная информация хранится на серверах организации – почтового сервиса в течение 6 месяцев с момента ее удаления.

*Также, в ходе расследования уголовного дела № 122012700130000**, расследуемого Следственной частью Следственного управления УМВД России по Калининградской области по обвинению Ш. в совершении преступлений, предусмотренных ч. 4 ст. 159, ч. 4 ст. 159 УК РФ, следователем получено судебное решение о производстве выемки в ООО «Яндекс» сведений о входящих, исходящих и удаленных сообщениях электронного почтового ящика nde******a@yandex.ru, однако произвести выемку сообщений не представилось возможным ввиду того, содержимое электронного почтового ящика было удалено, а с момента совершения преступления до момента возбуждения уголовного дела прошло более 2-х лет, а с момента возбуждения уголовного дела до момента обращения следователя с ходатайством о производстве выемки электронных сообщений прошло еще более 6 месяцев*[2].

Таким образом, учитывая продолжительность выявления преступления и длительность его расследования, можно констатировать тот факт, что та электронная доказательственная информация, которая могла, возможно, нести доказательственное значение, была безвозвратно утрачена. Вместе с этим, следуя разработанному нами алгоритму, описанному в параграфе 2.1 настоящего исследования, предписывающему о своевременности производства следственных действий, связанных со своевременной фиксацией электронной

[1] Из практики работы Следственной части по расследованию организованной преступной деятельности УМВД России по Калининградской области за 2022 г.

[2] Из практики работы Следственной части по расследованию организованной преступной деятельности УМВД России по Калининградской области за 2024 г.

доказательственной информации, возможно своевременно предотвратить утрату необходимой доказательственной информации, которая, в зависимости от обнаруженных электронных следов, может быть как положена в основу обвинения, так и использоваться в качестве дополнительных доказательств определенных событий или действий фигурантов по уголовному делу.

Возвращаясь к ранее приведенному примеру, связанному с утратой возможности провести выемку содержимого электронного почтового ящика, хочется акцентировать внимание на том, что уголовное дело по признакам двух преступлений, предусмотренных ч. 4 ст. 159 УК РФ, были возбуждены спустя более двух лет с момента совершения преступления. Таким образом, даже при соблюдении требований разработанного нами алгоритма, следователь также мог бы столкнуться с вопросом о том, что содержимое электронного почтового ящика пусто.

Как понимается, указанная переписка могла быть удалена и ранее, на период выявления и документирования указанных обстоятельств в ходе оперативно-розыскной деятельности, либо на этапе проведения проверки сообщения о преступлении в порядке ст.ст. 144-145 УПК РФ. В таких случаях, необходимо отметить следующее. Своевременное получение электронной доказательственной информации, в том числе посредством обращения в организации, осуществляющие администрирование электронными почтовыми сервисами, а также ее анализ может ускорить установление достаточных данных, указывающих на признаки преступления и определить круг лиц, причастных к совершению преступления, а также лиц, осведомленных о проверяемых событиях.

Обсуждая указанный вопрос, важно заострить внимание на том, что фактически органы, осуществляющие оперативно-розыскную деятельность, имеют право проводить оперативно-розыскные мероприятия по получению оперативным путём корреспонденции электронных почтовых ящиков, посредством проведения оперативно-розыскного мероприятия «Наведение

справок» или «Получение компьютерной информации», предварительно получая санкцию суда. Такое планирование организации проведения оперативно-розыскных мероприятий, при необходимости долгой разработки лиц или преступных групп, может способствовать более качественному дальнейшему доказыванию виновности определенных лиц в совершении преступлений и предотвратит возможность утраты значительно важных электронных следов преступлений, которые во многих случаях будет затруднительно установить в ходе расследования уголовного дела.

Помимо этого, в указанные выше организации, администрирующие электронные почтовые сервисы, социальные сети и мессенджеры, необходимо направлять следственные запросы о предоставлении регистрационных данных, которые указанным пользователем были указаны при регистрации аккаунта, почтового ящика, а также IP-адресов, с которых проходила регистрация, а также активация при отправлении сообщений[1]. Наличие указанных сведений в своей совокупности несет доказательственное значение, подтверждающее ведение переписки конкретным фигурантом.

Обращаясь к процессуальным нюансам производства выемки электронной переписки в организациях, обеспечивающих передачу электронных сообщений, можно отметить, что механизм, закрепленный в части 7 статьи 185 УПК РФ, касающийся вопросов изъятия электронных сообщений в учреждениях, предоставляющих услуги передачи информации через сети связи, вызывает значительное количество критики в области криминалистической науки.

Ряд ученых отмечает, что порядок, описанный в части 7 статьи 185 УПК РФ, закрепляющий порядок производства выемки электронных сообщений в организациях, обеспечивающих их передачу, не соответствует процедуре наложения ареста на почтово-телеграфные отправления, а также порядку их осмотра и выемки, как это подразумевается в статье 185 УПК РФ. Указанные

[1] См. об этом: Рамалданов Х.Х. Понятие и сущность цифровизации доказательств и доказывания в уголовном судопроизводстве // Вестник Волгоградской академии МВД России. - 2022. - № 1. - С. 121-128.

авторы считают, что вместо того чтобы дополнить этот порядок, он создает с ним противоречие. В качестве аргументов свей научной позиции, указанные авторы приводят доводы о том, что процесс обмена электронными сообщениями не допускает ареста самих сообщений и их физического изъятия, поскольку они представляют собой электронную информацию, а не предмет материального мира. В результате проведения следственных действий возможно лишь получение копий переписки с серверов организаций, которые обеспечивают передачу этих сообщений через электросвязь[1].

Обсуждаемый вопрос, по нашему мнению, является дискуссионным. В действительности, арест почтовых отправлений фактически связан с физическим задерживанием почтовых отправлений, их проверкой следователем в почтовом отделении и последующим принятием решения о копировании задержанной корреспонденции и дальнейшей отправке ее адресату. Вместе с тем указанный порядок изъятия почтовой корреспонденции совершенно не относится к процессу изъятия сообщений данного типа – электронных сообщений.

Основная идея отправки электронных сообщений заключается в их мгновенном обмене. Поэтому, на наш взгляд, разработка моделей для ареста, задержания и копирования информации в контексте традиционной почты нецелесообразна для данного типа сообщений.

Например, такие системы, как социальные сети и мессенджеры, имеют функции уведомления о доставке и прочтении сообщения. Следовательно, отсутствие таких уведомлений может вызвать подозрения у заинтересованных в исходе уголовного дела лиц, о возможном контроле их сообщений со стороны правоохранительных органов. Кроме того, переписка может продолжаться длительное время и в совокупности иметь доказательную значимость, в то время как изолированные фрагменты могут искажать полную картину происходящего.

---

[1] См. подробнее: Мещеряков В.А. «Виртуальные следы» под «Скальпелем Оккама» / Информационная безопасность регионов, Саратов, 2009

Кроме этого, следует отметить, что в части 7 статьи 185 УПК РФ отсутствует законодательно установленная возможность ареста электронных сообщений и данных, которые передаются через средства связи. В законодательстве лишь упоминается возможность их осмотра и выемки.

Несмотря на это, в области юриспруденции бытуют мнения ученых о том, что данная норма права не имеет достаточных оснований для ее законодательного закрепления именно в статье 185 УПК РФ. Это связано с невозможностью фактически арестовать упомянутую корреспонденцию, а также осуществить изъятие таких сообщений из-за их специфики. В этой связи некоторые исследователи предлагают создать и законодательно оформить новые следственные действия, которые на их взгляд более соответствовали бы целям и назначению их производства.

Так, например, А.И. Зазулин предлагает именовать следственное действие в ходе которого производится выемка электронных сообщений в организациях их передающих, как «Получение информации о соединениях между абонентами и (или) абонентскими устройствами, а также информации, содержащейся в сообщениях, передаваемых посредством сервисов электронной почты, обмена мгновенными сообщениями или иным подобным образом»[1], Т.И. Гарипов считает, что указанное следственное действие должно называться «Копирование и осмотр электронных сообщений и иных передаваемых по сетям электросвязи сообщений»[2], Е.В. Никитина и В.С. Раменская считают, что название данного

[1] См.: Зазулин А. И. Правовые и методологические основы использования цифровой информации в доказывании по уголовному делу: дис. ... канд. юрид. наук. Екатеринбург, 2018. 251 с.

[2] См. подробней: Гарипов Т.И. Вопросы процессуальной регламентации копирования и осмотра электронных сообщений в уголовном судопроизводстве // Вестник Казанского юридического института МВД России. 2019. Т. 10, No 4. С. 475-481. DOI: 10.24420/KUI.2019.79.74.012

[3] См. об этом: Никитина Е.В., Раменская В.С. Проблемы законодательного регулирования следственного действия, направленного на получение доступа к электронным сообщениям. // Российское право: образование, практика, наука. 2022. № 2. С. 25-32. DOI: 10.34076/2410_2709_2022_2_25.

следственного действия следует сформулировать как «Получение информации об электронных сообщениях, их копирование и осмотр»[1].

Тем не менее, несмотря на всесторонность и полноту вышеуказанных проведенных исследований, мы не разделяем мнения авторов. Считаем, что текущее законодательное определение следственного действия, связанного с изъятием электронных сообщений в ходе расследования преступлений непосредственно в организациях, осуществляющих их передачу, является наиболее емким и в то же время универсальным.

При анализе практики изъятия электронных писем и других данных, передаваемых через системы связи, необходимо выделить два основных этапа. Первый этап включает получение судебного решения, которое дает разрешение на изъятие электронных сообщений[2]. Второй этап состоит в фактическом изъятии в организации, которая обеспечивает обмен данными, на основании полученного судебного решения материального носителя информации, содержащего копии откопированных с серверов организации электронных сообщений[3].

Хотя упомянутый метод сбора доказательной информации связан с изъятием носителей с уже скопированными данными, мы считаем, что юридическое определение «выемка электронных сообщений», тем не менее, является наиболее корректным и универсальным. Это определение позволяет на основании судебных решений осуществлять как изъятие материальных носителей, содержащих как информацию, ранее скопированную с сервера, так и в необходимых случаях проводить изъятие электронных сообщений, находящихся на сервере организации, с помощью привлеченного специалиста посредством их перемещения с указанных серверов на иные носители информации. Также возможно изъятие данных с серверов организации с последующим ограничением

---

[2] См. подробнее: Малыгин К.В. Проблемы обеспечения Конституционных прав граждан в процессе изъятия электронной информации в уголовном судопроизводстве // Ex jure. 2023. №4.

[3] См. об этом: Архипова Н. А. Тактика осмотра и выемки электронных сообщений, передаваемых по сетям электросвязи // Закон и право. – 2018. – № 6. – С. 132–135.

доступа к ним для других лиц, включая сотрудников организации, обеспечивающей передачу данных через сети электросвязи. Таким образом, упомянутый способ получения доказательственной информации является более широким, чем просто копирование электронных сообщений, поскольку подразумевает не только «копирование», но и «перемещение» информации.

Выемка электронных сообщений, как описано выше, то есть посредством перемещения данных с серверов организации на другие электронные носители, может иметь место в тех ситуациях, когда необходимо получить электронные письма и информацию о них в компаниях, использующих свои домены электронной почты. Например, в крупных компаниях зачастую есть собственные корпоративные домены, которые контролируются самой организацией и располагают собственным сервером. Исключением из данной тенденции также не являются и государственные органы. В деятельности государственных органов, органов местного самоуправления, предприятий с государственным участием давно используются как специально разработанные системы электронного документооборота, так и собственные ведомственные сервисы электронной почты.

Возвращаясь к вопросам получения электронной доказательственной информации, в частности, применительно к расследованию преступлений в сфере экономики, следует акцентировать внимание на то, что фактически упомянутые выше почтовые сервисы администрируется сотрудниками указанных организаций и ведомственных учреждений. Рассматривая необходимость получения наиболее полных и достоверных доказательств, на наш взгляд, в ряде случаев можно поставить под сомнение полноту полученных данных в случае выбора тактики проведения указанного следственного действия посредством изъятия носителя информации с уже сохраненными на них данными, которые, соответственно подготовлены сотрудниками указанной организации или учреждения.

При таких обстоятельствах, выемка электронных сообщений путем выемки электронных носителей с сохраненными на них копиями электронных сообщений с серверов таких организаций, подготовленных при этом сотрудниками этих же организаций, будет на наш взгляд тактически неверным. Часто руководители этих структур не желают предоставлять следователю полное и объективное представление о корреспонденции в корпоративной почте. В результате, есть вероятность, что следователь получит искаженные или неполные сведения. Эти факторы вновь подтверждают тактическую целесообразность проведения данного следственного действия — *выемки* информации из электронных сообщений на почтовых ящиках организаций именно описанным выше способом *«перемещения».*

Юридическим основанием для изъятия указанных сообщений служит решение суда, так как данное следственное действие затрагивает право личности на тайну переписки. Известно, что ограничение конституционных прав граждан может осуществляться только на основании судебного решения. Мы поддерживаем научные подходы, которые утверждают, что изъятие электронных сообщений невозможно без наличия соответствующего решения суда[1].

В связи с этим мы полагаем, что для выемки электронных писем, фактически хранящихся на "корпоративных" почтовых серверах посредством их "перемещения", необходимо в ходатайстве перед судом обосновать и аргументировать целесообразность использования именно этого метода изъятия.

Мы полагаем, что не следует вводить законодательные ограничения на выбор тактики, которую следственные органы могут применять в ходе следственных действий в процессе получения сведений об электронных сообщениях в организациях, обеспечивающих их передачу. Сокращение

[1] См.: Симакова, Е. А. Особенности изъятия сведений, содержащихся в электронных сообщениях или иных передаваемых по сетям электросвязи сообщениях / Е. А. Симакова // Безопасность информационных технологий в правоохранительной сфере : Материалы международной научно-практической конференции, Санкт-Петербург, 11–12 мая 2023 года. – Санкт-Петербург: Санкт-Петербургский университет МВД РФ, 2023. – С. 51-54.

возможностей до простого копирования информации с серверов организаций, не является на наш взгляд оптимальным решением с учетом приведенных выше следственных ситуаций, при которых именно фактическое изъятие электронных сообщений позволит соблюсти объективность расследования и получение наиболее полных доказательств расследуемых преступлений.

Существуют проблемные аспекты, связанные с получением электронных сообщений от зарубежных организаций, которые предоставляют услуги передачи данных через сети связи, такие как Gmail, Telegram и иных[1]. Эти проблемы вызваны несколькими факторами, включая ограниченные сроки хранения данных на серверах компаний, которые соответствуют законодательным требованиям иностранных государств и международным нормам. Также имеет место использование так называемого «сквозного шифрования», при котором сообщения, отправляемые в чатах, фактически не хранятся. Дополнительно возникают трудности при обращении в компетентные органы зарубежных стран с запросами о правовой помощи в соответствии со статьей 453 УПК РФ. Эти сложности связаны как с длительностью процесса подачи и получения информации, так и с риском отказа в предоставлении данных, поскольку согласно международным договорам, заключенным с Россией, иностранные государства могут отклонить запросы по различным причинам. Например, если деяние не считается преступлением по их законодательству или если информация может повредить интересам иностранного государства.

Также, одним из оснований для направления запроса о правовой помощи компетентным органам иностранного государства в порядке ст. 453 УПК РФ является наличие международно-правового договора, заключенного РФ с иностранным государством. Основанием для отказа в исполнении запроса о правовой помощи может, как раз-таки являться отсутствие

[1] См. подробней: Костенко Н.С., Семененко Г.М., Пшеничкин А.А. Основные проблемы раскрытия и расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, на современном этапе // Вестник ВИ МВД России. 2020. №4.

международно-правового договора, в соответствии с которым иностранное государство обязуется исполнять запросы о международно-правовой помощи.

Кроме того, мессенджеры обладают особыми чертами и специально установленными правилами, которые регулируют основания, условия и способы взаимодействия с правоохранительными учреждениями. Пренебрежение такими нормами может привести к отказу зарубежного поставщика услуг в предоставлении запрашиваемой информации из-за её отсутствия.

Так, в рамках расследования уголовного дела против С., обвиняемого в совершении насильственных действий сексуального характера в отношении несовершеннолетнего (п. «б» ч. 4 ст. 132 УК), следователь ГСУ СК России по г. Москве направил запрос о правовой помощи в Соединенные Штаты. Это было необходимо для получения информации, важной для дела, которая хранилась в мессенджере Facebook. Эта социальная сеть принадлежит компании Meta, признанной в России экстремистской организацией и запрещённой на территории страны. Однако предоставленные сведения не были получены от провайдера услуг, который заявил о том, что информация отсутствует в базе данных Facebook, а предварительный запрос на сохранение данных не был отправлен[1].

Указанный пример в очередной раз иллюстрирует необходимость комплексного подхода к получению электронной доказательственной информации, хранимой в электронных переписках. В частности, последняя свидетельствует о необходимости на первоначальном этапе расследования как обеспечения возможности получения доказательственной информации от организаций, обеспечивающих обмен сообщениями, так и о необходимости принятия своевременных мер по отысканию, изъятию и последующей фиксации доказательственной информации, содержащейся в электронных носителях информации. В том числе посредством проведения таких следственных действий как осмотр и проведение компьютерно-технической судебной экспертизы.

[1] Из практики работы ГСУ СК России по г. Москве за 2023 г.

Таким образом, при проведении выемки переписки в организациях операторов и провайдеров, следует учитывать следующие особенности таких следственных действий. В ходатайстве о выемке перед судом необходимо указывать, что изъятию подлежит как *имеющейся* на электронном почтовом ящике переписка, так и *удаленная* с него; необходимо помнить, что удаленная переписка очищается в серверов электронных почтовых сервисов по истечению 6 месяцев с момента ее удаления пользователем; важно запрашивать сведения о регистрационных данных, которые указывались пользователями при регистрации аккаунта.

Помимо этого, при возникновении сомнений в незаинтересованности представителей организаций, в которых проводится выемка, в необходимых случаях, в том числе и в ведомственных или корпоративных сервисах электронной почты, выемку электронных сообщений проводить посредством их «перемещения», а не «копирования».

2.5 Специфика использования специальных знаний при расследовании преступлений в сфере экономики, совершенных с использованием информационных технологий

Анализируя вопросы применения информационных технологий следователями при расследовании преступлений, в том числе в сфере экономики, нельзя не затонуть вопросы применения специальных познаний экспертами и специалистами в области получения доказательственной информации по данной категории преступлений[1].

В массиве всех назначаемых судебных экспертиз при расследовании преступлений данной категории, довольно большой пласт занимают компьютерно-технические судебные экспертизы. Помимо этого, в ходе расследования преступлений в сфере экономики, довольно часто следователи прибегают к помощи специалистов, обладающими специальными познаниями в области информационных технологий. Такое взаимодействие происходит как посредством привлечения специалиста к участию в следственных действиях, связанных с изъятием электронных носителей информации (обыски, выемки и другие), так и к участию в следственных действиям, связанных с их дальнейшим исследованиям (осмотры предметов).

Компьютерно-техническая экспертиза – это исследование цифровых устройств и данных для установления фактов, связанных с их использованием.

---

[1] См. об этом: Мещеряков В. А. Особенности специальных знаний, используемых в цифровой криминалистике / В. А. Мещеряков // Известия Тульского государственного университета. Экономические и юридические науки. – 2013. – № 4–2. – С. 88; Семикаленова, А. И. Цифровые следы: неожиданные проблемы исследования / А. И. Семикаленова // Цифровой след как объект судебной экспертизы: Материалы Международной научно-практической конференции, Москва, 17 января 2020 года. – Москва: РГ-Пресс, 2023. – С. 195-197. – EDN ONOGNK; Россинская, Е. Р. Учение о цифровизации судебно-экспертной деятельности и проблемы судебно-экспертной дидактики / Е. Р. Россинская // Правовое государство: теория и практика. – 2020. – № 4–1(62). – С. 88–101.

Основные задачи компьютерно-технической экспертизы включают извлечение, восстановление, анализ и интерпретацию информации, хранящейся на компьютерах, мобильных телефонах и других электронных носителях информации[1]. Говоря об объектах исследования, следует отметить, что ими могут являться: аппаратное и программное обеспечение, носители информации, цифровые следы, оставленные пользователями[2]. В результате проводимых исследований КТЭ позволяет реконструировать обстоятельства совершения преступления, определить время и способ доступа к данным, и как результат в совокупности с иными доказательствами по делу подтвердить причастность лиц к совершению преступлений.

Вместе с этим, говоря о применении информационных технологий при производстве исследований и экспертиз нельзя говорить только о том, что последние применяются исключительно для проведения судебных компьютерно-технических экспертиз.

Информационные технологии используются и для проведения иных экспертиз, в числе которых фоноскопическая, видеотехническая судебные экспертизы, судебно-экономическая судебная экспертиза и иные.

Говоря о фоноскопической и видеотехнической экспертизах, следует отметить, что они занимаются анализом звуковых и видеозаписей для установления подлинности, идентификации участников и реконструкции событий. Современные методы включают цифровое шумоподавление, спектральный анализ, сравнение голосов и изображений, а также визуализацию скрытых деталей. При производстве данных исследований эксперты анализируют

---

[1] См. подробней: Мещеряков, В. А. Формирование дополнительных компетенций экспертов криминалистических экспертиз в сфере исследования информационных систем и компьютерных устройств / В. А. Мещеряков, Ю. М. Баркалов // Вестник Воронежского института МВД России. – 2020. – № 1. – С. 183-188.

[2] См. об этом: Мещеряков В.А. Копирование информации с компьютерных носителей при производстве следственных действий / В. А. Мещеряков, О.Ю. Цурлуй // Цифровой след как объект судебной экспертизы: Материалы Международной научно-практической конференции, Москва, 17 января 2020 года. – Москва: РГ-Пресс, 2021. – С. 128-132.

акустические и визуальные характеристики, чтобы выявить признаки монтажа, подделки или фальсификации. Таким образом, применение современных информационных технологий способствуют проведению данных экспертиз по уголовному делу в целях обеспечения объективных и достоверных доказательств.

Современные информационные технологии используются и при проведении судебно-экономической экспертизы[1]. При проведении данной экспертизы используется специализированное ПО для извлечения, восстановления и анализа информации из сложных информационных систем. Они проверяют корректность отражения операций, соответствие законодательству и выявляют признаки искажений (при необходимости).

Применение современных информационных технологий при проведении судебно-экономических экспертиз заключается в автоматизации, повышении точности и ускорении анализа больших объемов сложных финансовых данных, представленных в электронном виде. Современные информационные технологии позволяют: эффективно обрабатывать и анализировать электронные документы, сокращая при этом время, помимо этого технологии активно работают с анализом электронных файлов, базами данных, ERP-системами, что значительно ускоряет процесс. Кроме этого, информационные технологии позволяют сохранять целостность и доказательств: создавать цифровые копии (образы) данных, что предотвращает возможность внесения в них изменений. Кроме этого, информационные технологии позволяют наглядно представлять финансовую информацию в виде графиков, диаграмм, таблиц, что облегчает восприятие участниками процесса, включая и суд.

---

[1] См. об этом: Шапиро Л. Г. Судебно-экономические экспертизы в борьбе с преступностью в сфере экономики: процессуальные и криминалистические проблемы / Л. Г. Шапиро // Вестник Саратовской государственной юридической академии. - 2016. - № 1. - С. 158-163. - Библиогр. в сносках. - полный текст статьи см. на сайте Научной электронной библиотеки https://elibrary.ru . - ISSN 2227-7315.

Таким образом, современные информационные технологии трансформируют судебно-экономическую экспертизу, делая ее более объективной, быстрой, точной и глубокой.

Для автоматизированного анализа данных, выявления скрытой информации, восстановления удаленных файлов экспертами и специалистами используется специализированное программное обеспечение.

Так, например, для фоноскопической экспертизы (анализ звуковых записей) используются такие комплексы для цифровой обработки звука Lexichen (предназначен для идентификации, сравнения и анализа речи, а также выявления признаков монтажа), "Мультиспектр" и "Анализатор" (используются для спектрального анализа, идентификации голоса, определения наличия посторонних шумов и признаков монтажа), Adobe Audition / Sound Forge (для первичной обработки, шумоподавления), ASR - Automatic Speech Recognition (применятся в качестве вспомогательного средства для транскрибирования записей, что помогает в дальнейшем анализе текста)[1].

Для видеотехнической экспертизы (анализ видеозаписей) используются такие программные средства как "ВидеоДок" / "Видеотест" (российские программные комплексы, предназначенные для анализа видеозаписей, установления фактов монтажа, идентификации объектов и субъектов, восстановления утраченной информации), VLC Media Player, Adobe Premiere Pro / After Effects (программы-видеоредакторы, которые могут использоваться для детального покадрового анализа, сравнения различных фрагментов, выявления признаков цифрового монтажа, цветокоррекции, анализа движения), Regard: Программный комплекс, часто используемый для анализа видеодоказательств, определения времени и последовательности событий. Также при проведении видеотехнической экспертизы используется программное обеспечение для

[1] См. подробней: Лебедева А. К. Проблемы производства судебной фоноскопической экспертизы в свете развития цифровых технологий // Вестник Университета имени О. Е. Кутафина. 2020. №6 (70); Неупокоева И.А. Назначение судебной фоноскопической экспертизы при расследовании мошенничества с использованием информационно-коммуникационных технологий // Закон и право. 2021. №3.

распознавания лиц и объектов, системы, основанные на нейронных сетях, которые могут использоваться для идентификации лиц, транспортных средств, других объектов на видеозаписи, инструменты для анализа метаданных (информации о камере, времени съемки, настройках, месте съемки, содержащуюся в файлах изображений и видео)[1].

При проведении компьютерно-технических судебных экспертиз, исследований, а также в ходе производства осмотров предметов, объектом которых являются электронные носители информации, специалистами и экспертами, в частности экспертно-криминалистических подразделений МВД России, в основном применяется в деятельности аппаратно-программный комплекс «Мобильный Криминалист».

«Мобильный Криминалист» — это настольное приложение, предназначенное для извлечения данных из мобильных телефонов и смартфонов. Эта программа стала важным инструментом в расследованиях уголовных и правонарушений более чем в 20 странах. Главная задача программы заключается в сборе информации, которая может служить доказательством в судебном процессе. Теперь она доступна и на русском языке в России.

Программа активно используется по всему миру различными государственными учреждениями, правоохранительными органами, военными и налоговыми службами. Мобильные устройства содержат ценную информацию, включая контакты, историю звонков, аудиозаписи, фотографии и многие другие данные.

«Мобильный Криминалист» может извлекать обширные данные из телефона без сложного оборудования, поддерживая более 300 моделей устройств. Анализ данных можно проводить как непосредственно в программе, так и с помощью экспорта в популярные форматы файлов. Программа гарантирует

[1] См. подробней: Подволоцкий И. Н. Перспективы комплексного исследования портретных видеоизображений судебными экспертами // Актуальные проблемы российского права. 2018. №12 (97).

сохранность информации на мобильных устройствах, обеспечивая парольную защиту.

С интерфейсом на русском языке и поддержкой Unicode, «Мобильный Криминалист» предлагает эффективные инструменты для работы с данными мобильных устройств[1].

Вместе с этим, несмотря на довольно широкие возможности аппаратно-программных комплексов, используемых в судебно-экспертных экспертных учреждениях Российской Федерации, современные информационные технологии развиваются ежедневно, в связи с чем, имеется необходимость и постоянного совершенствования технических средств, состоящих на «обеспечении» судебно-экспертных учреждений[2].

Важно учитывать, что при анализе доказательственно-значимой информации, сохраненной на электронных носителях информации имеется ряд обстоятельств, которые важно учитывать при совершенствовании технических средств, предназначенных для фиксации и закрепления таких следов[3].

Так трудности возникают при анализе сильно поврежденных устройств, к примеру, утопленных, сгоревших, разбитых, которые невозможно включить, подключить или восстановить их основные компоненты. При таких ситуациях при проведении судебной экспертизы потребуются манипуляции, связанные с извлечением плат, чипов и их последующий анализ, что существенно отражается как на сроках проведения экспертизы, так и на количестве информации, которую удастся восстановить.

---

[1] Российские следователи-криминалисты используют инновационное ПО для раскрытия преступлений | IT Russia URL: https://itrussia.media/ru/article/rossiyskie-sledovateli-kriminalisty-ispolzuyut-innovatsionno?ysclid=mj68la99v036453868 (дата обращения: 20.11.2025).

[2] См. об этом: Бутенко О.С. Криминалистические и процессуальные аспекты проведения осмотра мобильных телефонов в рамках предварительного следствия // Lex Russica. 2016. №4 (113).

[3] См.: Россинская, Е. Р. Тренды развития криминалистики в условиях цифровой трансформации современной преступности / Е. Р. Россинская // Союз криминалистов и криминологов. – 2025. – № 1. – С. 162-173. – DOI 10.31085/2310-8681-2025-1-240-162-173. – EDN GPXCUA.

Кроме того, новейшие смартфоны (последние версии iPhone и Android) используют полнодисковое шифрование. Так, к примеру, в случае если устройство заблокировано надежным, сложным паролем/PIN-кодом/графическим ключом, и этот пароль неизвестен, то программы для мобильной криминалистики могут быть не в состоянии его обойти. Некоторые уязвимости обнаруживаются, но производители постоянно закрывают их. После нескольких неудачных попыток ввода пароля многие устройства самоудаляются или блокируются на более длительный срок, делая невозможным доступ к информации. Кроме этого, в условиях непрерывной модернизации систем безопасности, мобильными производителями, последние модели устройств и обновления ОС регулярно внедряют усиленные протоколы защиты, не имеющие публично доступных или коммерческих уязвимостей на момент их релиза. Следовательно, специалистам по разработке криминалистических инструментов требуется период для возможности создания методик обхода этих новых защитных механизмов[1].

Также важно отметить, что одной из проблем поиска электронных следов на изъятом электронном носителе информации может служить полный сброс данных устройства до заводских настроек либо данные были перезаписаны, то восстановление стертых данных представляется весьма затруднительным с технической стороны, иногда и вовсе невозможным.

Немало важной проблемой в контексте поиска электронной следовой картины преступлений на своевременном этапе, что характерно также и для преступлений в сфере экономики, является проблема поиска данных, хранящихся в облачных хранилищах. Так, при анализе памяти устройства, данная информация не может быть обнаружена, поскольку она находится на удалении и не хранится на устройстве (хранится только в облачных сервисах (iCloud, Google Drive и т.д.), и соответственно требует отдельных процедур получения данных у провайдеров и не может быть извлечена с устройства, если ее локальной копии не имеется.

---

[1] См. подробней: Камышев С.В., Карманов И.Н. Мобильная криминалистика: задачи и технологии // Интерэкспо Гео-Сибирь. 2018. №7.

Таким образом, программа "мобильный криминалист" и ее аналоги, используемые экспертами и специалистами при извлечении доказательственной важной информации с электронных носителей является весомым, но не всемогущим инструментом в поиске «электронных» следов преступлений, как и в целом, проведение компьютерно-технических экспертиз и исследований в рамках уголовных дел. При поиске, фиксации и закреплении таких доказательств важен комплексный подход, который заключается в одновременном поиске информации как на вещественных доказательствах – электронных носителях, в том числе с использованием специальных знаний, так и поиск информации, хранящейся на удаленных серверах провайдеров, организаций обеспечивающих обмен и передачу электронных сообщений[1].

Делая общий вывод о проблемах использования специальных знаний при расследовании преступлений в сфере экономики, совершенных с использованием информационных технологий, следует отметить, что таковыми являются: динамичное развитие технологий, в том числе и связанных с современными способами хранения информации (облачные сервисы), ее получении (искусственный интеллект), новых способах оплаты (бесконтактная с использованием NFC, с использованием QR-кодов), даже новых «валют» (криптовалюта) и методов совершения преступлений, что требует постоянного обновления знаний и методик экспертизы. Кроме этого - огромные массивы информации, сложность извлечения, анализа, а также легкость модификации, удаления или шифрования цифровых следов. Также важно отметить как одной из проблем отставание правовой базы: необходимость постоянного анализа регулирования на законодательном уровне вопросов, связанных с фиксацией электронных следов – вопросов изъятия и копирования информации с электронных носителей, учитывая их техническую составляющую, и проведения

[1] См.: Майлис Н. П. Использование информационных ресурсов при производстве судебных экспертиз / Н. П. Майлис // Вестник экономической безопасности. – 2021. – № 3. – С. 166–169.

исследований с использованием специальных знаний в отношении последних. Высокая стоимость и ресурсоемкость экспертиз, что связано с необходимостью использования современного дорогостоящего оборудования, специализированного программного обеспечения и привлечения высокооплачиваемых экспертов[1].

Решение вышеуказанных проблем, связанных с применением специальных знаний при расследовании преступлений в сфере экономики заключается в применении комплексного подхода, связанного с широким внедрением в деятельность эксперта и специалиста информационных технологий, правового регулирования и правоприменительной практики в данной сфере.

В частности:

1. Для решения проблемы эффективного извлечения и анализа больших объёмов данных, необходимо совершенствование аппаратно-программных комплексов, используемых специалистами и экспертами при проведении исследований.

Необходимо постоянно совершенствовать аппаратно-программные комплексы, используемые специалистами и экспертами при проведении исследований[2]. В частности, позволяющие извлекать анализа большие объёмы данных (Big Data), проводить комплексный анализ движений денежных средств по различным счетам организаций, анализировать данные из облачных хранилищ.

Требуется создание новых методик проведения исследований и экспертиз исходя из уровня развития технологий и современных платежных систем и систем бухгалтерского учета.

---

[1] См. об этом: Камышев С.В., Карманов И.Н. Мобильная криминалистика: задачи и технологии // Интерэкспо Гео-Сибирь. 2018. №7.

[2] См. об этом: Наумов А. Е., Юдин Д. А., Долженко А. В. Совершенствование технологии проведения строительно-технических экспертиз с использованием аппаратно-программного комплекса автоматизированной дефектоскопии // Вестник БГТУ имени В.Г. Шухова. 2019. №4.

2. Для автоматизации рутинных операций целесообразна разработка программ по использованию искусственного интеллекта и машинного обучения. Исходя из этого требуется внедрение междисциплинарных образовательных программ для экспертов, объединяющих знания в области юриспруденции, экономики, бухгалтерского учета и современных информационных технологий.

Необходимо совершенствовать уровень профессионального развития специалистов, экспертов, проводящих различные исследования при расследовании преступлений данной направленности[1]. Совершенствование уровня профессионального развития заключается в разработке и во внедрении междисциплинарных образовательных программ для экспертов, объединяющих знания в области юриспруденции, экономики, бухгалтерского учета и современных информационных технологий (в том числе и криптоанализ, облачные технологии).

[1] См. об этом: Орлова Т.В., Бушуев В.В. Формирование и развитие профессиональных компетенций судебного эксперта в области криминалистического исследования документов и портретной экспертизы // Вестник Московского университета МВД России. 2023. №2.

ЗАКЛЮЧЕНИЕ

В результате проведенного исследования мы пришли к следующим результатам и выводам.

В целях перехода к унифицированному языку права, основными признаками которого являются точность, ясность, использование слов и терминов в строго определенном смысле, представлены определения понятий «информационные технологии», «информационно-коммуникационные технологии» и «цифровые технологии».

Информационные технологии определяются как технологии, используемые в процессе собирания, обработки, накопления и передачи криминалистически значимой информации, при функционировании которых происходит образование информации нового качества о состоянии объекта, процесса или явления.

«Информационно-коммуникационные технологии» является меньшим по объему, чем понятие «информационные технологии», так как является частью инфраструктуры информационных технологий, который заключается именно в коммуникации – обмене информацией и определяется как инфраструктура передачи данных по ее каналам и связанная с ней обработка информации.

Цифровые технологии являются подвидом информационных технологий и определяются как технологии, использующие совокупность средств и методов собирания, обработки, накопления и передачи криминалистически значимой информации сбора, обработки, накопления и передачи данных (первичной информации) для получения информации нового качества о состоянии объектов, процессов, явлений с использованием цифрового (двоичного) кода.

Основными признаками информационных технологий являются направленность на обработку информации, что выражается в автоматизации рутинных операций и использование технических средств (аппаратное обеспечение). Данный признак выражается в том, что технические средства опираются на физические устройства

Классифицируя информационные технологии по системам исчисления лежащим в основе, можно выделить компьютерные информационные

технологии и не связанные с компьютерными (не основанные на двоичной системе). Обращаясь к классификации информационных технологий по типу решаемых задач: технологии обработки данных; технологии управления; офисные технологии; экспертные технологии. Классифицируя информационные технологии по возможностям взаимодействия между собой можно выделить локальные информационные технологии, сетевые информационные технологии, облачные информационные технологии. Классифицируя информационные технологии по сфере применения применительно к процессу расследования преступлений, выделяются криминалистические информационные технологии, информационные технологии в финансовой сфере и геоинформационные технологии.

Для систематизации и анализа видов современных информационных технологий, используемых в юриспруденции необходимо выделение видов информационных технологий, необходимо выделение видов информационных технологий, используемых и при расследовании преступлений в сфере экономики: информационно-справочные и аналитические системы; системы электронного документооборота и управления следственным процессом; информационные технологии, предназначенные для поиска и фиксации криминалистически значимой информации; информационные технологии, используемые для коммуникации и дистанционного взаимодействия.

Нами выделены и основные направления использования информационных технологий в следственной практике. К ним отнесены следующие: использование информационно-справочных и аналитических систем для поиска информации; использование информационных технологий, предназначенных для фиксации следовой картины преступлений (средства сбора, фиксации и исследования доказательств); использовании информационных технологий для коммуникации и дистанционного взаимодействия; использование технологий для организации предварительного следствия (программные комплексы для ведения электронного дела, использование синхронных переводчиков, нейросетей); использование

технологий систем для электронного документооборот и управления следственным процессом.

Отличительными особенностями преступлений в сфере экономики, следует выделить несколько основных характеристик.

Во-первых, это причинение ущерба от преступлений. Указанные преступления обладают высокой латентностью, что связано с интеллектуальным характером их совершения, сокрытия и маскировки. Основные действия, направленные на совершение таких преступлений происходят как в административных зданиях, в офисах, кредитных учреждениях, равно как и могут совершаться удалено и дистанционно с доступом в сеть Интернет, в том числе используя интернет-банкинг для совершения платежей. Кроме этого, преступные действия часто маскируются под законные операции, проводимые в рамках гражданско-правовых отношений или регулируемые специальными нормативными актами.

Следовая картина данных преступлений выражена в сочетании идеальных и материальных следов, в том числе «электронных». Электронные следы – это данные о доступе к информационным системам, электронные документы, в том числе и сведения из Интернет-банкинга, платежные поручения, сформированные с их помощью сведения о движении денежных средств по счетам, электронная переписка, метаданные файлов. Данные следы в числе материальных следов обладают важным значением, ведь они преобладают в настоящее время над иными материальными следами, поскольку те же финансовые документы, о которых шла речь выше, хранятся в электронном виде.

В целях наиболее эффективной фиксации электронных следов на первоначальном этапе расследования преступлений в сфере экономики, разработан алгоритм первоначальных следственных действий при расследовании преступлений в сфере экономики, включающий комплекс следственных действий как направленных на отыскание электронных носителей информации, которые

могут содержать интересующие следствие данные, так и получение электронных следов из альтернативных источников.

Аргументирована необходимость проведения выемки сообщений электронной почты, переписки в социальных сетях в организациях, обеспечивающих передачу сообщений по сетям электросвязи на первоначальном этапе расследования преступлений, что в ситуациях, при которых констатировано удаление части сообщений, обеспечит установление удаленных сообщений, хранящихся на серверах соответствующей организации.

Выявлены и проанализированы проблемы применения информационных технологий, имеющие место при фиксации следовой картины преступлений.

На основе анализа мнений ученых и уголовных дел, при которых проводились следственные действия, направленные на изъятие электронных носителей информации, сделан вывод о том, что институт понятых не должен являться обязательным применительно к процессу изъятия и копирования информации с электронных носителей информации. При этом стоит ограничиться обязательностью их привлечения только к тем следственным действиям, их участие в которых обязательно в силу требований закона (например, обыск). Необходимость в участии понятых при производстве копирования информации с электронных носителей отсутствует, поскольку при копировании информации, сведения о скопированной информации, а именно о времени, дате, устройстве, с которого была скопирована информация, отображаются в свойствах скопированного файла. При этом, указанные сведения довольно затруднительно зафиксировать участвующему в ходе следственного действия понятому.

Аналогичный вывод сделан вывод о целесообразности исключения в законе обязательности привлечения к следственным действиям, связанным с изъятием электронных носителей информации либо копированием с них электронной доказательственной информации специалиста. По нашему мнению требуется установить возможность его привлечения по инициативе следователя или лица,

осуществляющего дознание, который должен сделать указанный вывод исходя из сложности электронного носителя информации, подлежащего изъятию.

Проанализированы и выделены особенности производства криминалистической видеосъёмки, фотофиксации при расследовании различных преступлений в сфере экономики, а также подчеркнута значимость поиска доказательственной информации, находящихся в открытом доступе в сети Интернет при расследовании преступлений в сфере экономики.

В ходе проведенного исследования на основе анализа эмпирического материала выявлены особенности производства допроса с использованием систем видео-конференц-связи – тактические и организационные. Автором разработаны практические рекомендации проведения допросов с использованием видео-конференц-связи при расследовании преступлений в сфере экономики.

Сделан вывод о том, что использование дистанционных технологий для допросов представляет собой современный правовой инструмент, способствующий оптимизации расследования преступлений, а также облегчает организацию допросов с участниками процесса, находящимися далеко от места совершения преступления.

Обоснована необходимость технического оснащения следственных органов необходимыми техническими средствами для организации проведения удаленных допросов в целях решения проблемы популяризации проведения следственных действий с использованием средств видео-конференц-связи и их внедрения в повсеместную работу следственных подразделений.

Автором проанализированы аспекты изъятия электронных носителей информации при расследовании преступлений в сфере экономики и разработаны рекомендации законодательного расширения оснований для изъятия электронных носителей информации.

Так, предлагается расширить законодательные основания для изъятия, в частности, дополнив статью 164.1 УПК РФ пунктом, разрешающим изъятие носителей при технической невозможности копирования данных, при наличии

соответствующего заявления специалиста. Вместе с этим в целях предотвращения возможных злоупотреблений со стороны следственных органов и защиты прав граждан и организаций, автор рекомендует установить временные рамки для осмотра изъятых носителей, признания их вещественными доказательствами и проведения экспертизы (при необходимости).

В ходе изучения аспектов осмотра электронных носителей информации при расследовании преступлений в сфере экономики, автором отмечено, что организация и проведение осмотра электронных устройств является сложным процессом, особенности которого проявляются как на стадии подготовки, так и в ходе самого следственного действия.

Подготовка к осмотру включает привлечение эксперта, определение места проведения и обеспечение необходимым оборудованием и программным обеспечением.

Осмотр электронных устройств осложняется наличием в современных гаджетах функций, таких как режим гибернации, удаленная блокировка и другие системы защиты информации, которые могут препятствовать всестороннему исследованию. Акцентировано внимание на необходимость проведения осмотра согласно разработанному определенному алгоритму действий, учитывающему уникальные свойства исследуемого объекта.

В случаях, когда искомая информация сохранена в облачных хранилищах - целесообразно зафиксировать их содержимое фотографированием, видеосъемкой или копированием данных — пока устройство подключено к интернету во время изъятия. После этого рекомендуется перевести устройство в режим полёта.

Также существуют специфические черты осмотра на активном этапе следственного действия, которые обусловлены наличием в современных гаджетах режима «гибернации» и функции удаленной блокировки. Более того, в отличие от осмотра других материалов и документов, данный тип осмотра следует проводить согласно определенному алгоритму действий, учитывающему уникальные свойства исследуемого объекта, которому необходимо следовать.

В частности, при осмотре и анализе мобильных устройств, в которых функционально предусмотрено использование e-sim необходимо следовать предложенным рекомендациям. При изъятии электронных носителей информации, посредством которых может быть осуществлен выход в сеть Интернет, следует отключать функции «передачи данных», активировать режим «в самолете»; извлекать стандартную сим-карту из слота изымаемого устройства; а в случае невозможности, незамедлительно выключать мобильный телефон.

При наличии риска утраты доказательственной информации при включении устройства, а также удаления или искажения данных, необходимо привлекать к участию в следственном действии специалиста, обладающего специальными познаниями в области радиотехники в целях применения им специальных устройств, предназначенных для подавления связи.

В ходе исследования автором выделены особенности получения электронной информации о переписках, содержащейся в электронной почте и мессенджерах, а также представлены рекомендации по их получению при проведении расследования.

Автором отмечены следующие нюансы:

- в ходатайстве перед судом о производстве выемки необходимо указывать, что изъятию подлежит как *имеющейся* на электронном почтовом ящике переписка, так и *удаленная* с него;

- важно провести выемку как можно скорее с момента возбуждения уголовного дела - удаленная переписка очищается в серверов электронных почтовых сервисов по истечению 6 месяцев с момента ее удаления;

- необходимо наряду с изъятием электронной переписки истребовать сведения о регистрационных данных, которые указывались пользователями при регистрации аккаунта;

- при возникновении сомнений в незаинтересованности представителей организаций, в которых проводится выемка - выемку электронных сообщений, фактически сохраненных на «корпоративных» почтовых серверах проводить

посредством их «перемещения», а не привычного распространенного «копирования».

При проведении оперативно-розыскной деятельности направленной на документирования рассматриваемого вида преступлений – своевременно планировать мероприятия по получению оперативным путём корреспонденции электронных почтовых ящиков.

Помимо изложенного, автором изучены проблемы получения электронной информации о переписках, содержащейся в ведомственных или корпоративных сервисах электронной почты, и на основе анализа представлены практические рекомендации по совершенствованию правоприменительной практики в указанном направлении изъятия электронной переписки, с учетом ее специфических особенностей.

По результатам анализа проблем использования специальных знаний при расследовании преступлений в сфере экономики предложены следующие меры по их решению.

1. Необходимо совершенствовать уровень профессионального развития специалистов, экспертов, проводящих различные исследования при расследовании преступлений данной направленности.

2. Необходимо постоянно совершенствовать аппаратно-программные комплексы, используемые специалистами и экспертами при проведении исследований.

3. Необходимо планомерное создание новых методик проведения исследований и экспертиз исходя из развития технологий и современных платежных систем, систем бухгалтерского учета, а также использования искусственного интеллекта и машинного обучения для автоматизации рутинных операций, анализа огромных массивов данных и поиска скрытых связей.

4. Постоянная актуализация и совершенствование нормативно-правовой базы в соответствии с вызовами современной техники.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

I. Нормативно-правовые и иные акты

1. Конституция Российской Федерации от 12 декабря 1993 г. (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС «Консультант Плюс».

2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 31.07.2025) // СПС «Консультант Плюс».

3. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 31.07.2025) // СПС «Консультант Плюс».

4. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 51-ФЗ (ред. от 31.07.2025, с изм. от 25.11.2025) // Собрание законодательства Российской Федерации — 1994. — № 32.

5. Арбитражный процессуальный кодекс Российской Федерации от 24.07.2002 N 95-ФЗ (ред. от 15.12.2025).

6. Жилищный кодекс Российской Федерации от 29.12.2004 № 188-ФЗ // Собрание законодательства Российской Федерации. — 2005. — № 1 (ч. I). — Ст. 14.

7. Федеральный закон «О полиции» № 3-ФЗ от 07 февраля 2011 г. (ред. от 15.12.2025) // СПС «Консультант Плюс».

8. Федеральный закон «О государственной судебно-экспертной деятельности в Российской Федерации» № 73-ФЗ от 31 мая 2001 г. (в ред. от 22.07.2024) // СПС «Консультант Плюс».

9. Федеральный закон «Об оперативно-розыскной деятельности» № 144-ФЗ от 12 августа 1995 г. (ред. от 01.04.2025) // СПС «Консультант Плюс».

10. Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006 (ред. от 24.06.2025) // СПС «Консультант Плюс».

11. Основы законодательства Российской Федерации о нотариате от 11.02.1993 № 4462-1 [Электронный ресурс] // СПС «Гарант». — Режим доступа: https://base.garant.ru/10102426/.

12. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // Собрание законодательства Российской Федерации. — 2003. — № 28. — Ст. 2895.

13. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. — 2006. — № 31 (ч. I). — Ст. 3448/

14. Федеральный закон от 05.04.2013 N 44-ФЗ (ред. от 26.12.2024) "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд" (с изм. и доп., вступ. в силу с 01.07.2025).

15. Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // Собрание законодательства Российской Федерации. — 2001. — № 33 (ч. I). — Ст. 3418.

16. Федеральный закон от 13.07.2015 № 218-ФЗ «О государственной регистрации недвижимости» // Собрание законодательства Российской Федерации. — 2015. — № 29 (ч. I). — Ст. 4344.

17. Федеральный закон от 24.07.2007 № 221-ФЗ «О кадастровой деятельности» // Собрание законодательства Российской Федерации. — 2007. — № 31. — Ст. 4017.

18. Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» // Собрание законодательства Российской Федерации. — 2010. — № 31. — Ст. 4179.

19. Федеральный закон от 30.12.2004 № 214-ФЗ «Об участии в долевом строительстве многоквартирных домов и иных объектов недвижимости и о внесении изменений в некоторые законодательные акты Российской Федерации»

// Собрание законодательства Российской Федерации. — 2005. — № 1 (ч. I). — Ст. 40.

20. Федеральный закон от 08.08.2024 № 222-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» [Электронный ресурс] // СПС «Гарант». — Режим доступа: https://www.garant.ru/products/ipo/prime/doc/409393099/.

21. Федеральный закон от 20.10.2022 № 408-ФЗ «О внесении изменений в статью 26 Федерального закона «О банках и банковской деятельности» и статью 27 Федерального закона «О национальной платежной системе» // Собрание законодательства Российской Федерации. — 2022. — № 43. — Ст. 7271.

22. Федеральный закон от 29.11.2012 № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» // Собрание законодательства Российской Федерации. — 2012. — № 49. — Ст. 6752.

23. Федеральный закон от 29.07.2017 № 245-ФЗ «О внесении изменений в Федеральный закон «О связи» // Собрание законодательства Российской Федерации. — 2017. — № 31 (ч. I—II). — Ст. 4794.

24. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V (с изменениями и дополнениями по состоянию на 16.09.2025 г.) [Электронный ресурс] URL: https://online.zakon.kz/Document/?doc_id=31575852&ysclid=mka4ej38o0930641777

25. Указ Президента РФ от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» // Собрание законодательства Российской Федерации. — 2024. — № 20. — Ст. 2584.

26. Указ Президента РФ от 22.05.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации». Доступ из справ. правовой системы «КонсультантПлюс».

27. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Доступ из справ. правовой системы «КонсультантПлюс».

28. Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации». Доступ из справ. правовой системы «Консультант Плюс».

29. Указ Президента РФ от 02.07.2021 № 400 «О стратегии национальной безопасности Российской Федерации». Доступ из справ. правовой системы «КонсультантПлюс».

30. Указ Президента РФ от 09.05.2017 № 203 «О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы. Доступ из справ. правовой системы «КонсультантПлюс».

31. Постановление Правительства РФ от 26.10.2012 № 1101 «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети “Интернет” и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети “Интернет”, содержащие информацию, распространение которой в Российской Федерации запрещено». Доступ из справ. правовой системы «КонсультантПлюс».

32. Постановление Правительства РФ от 23.12.2006 № 32 «Об утверждении правил оказания услуг по передаче данных». Доступ из справ. правовой системы «КонсультантПлюс».

33. Постановление Правительства РФ от 31.07.2014 № 743 «Об утверждении «Правил взаимодействия организаторов распространения информации в информационно-телекоммуникационной сети Интернет с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации».

34. Приказ МВД России от 03.04.2018 № 196 «О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений» [Электронный ресурс] // Режим доступа: https://xn--n1aicc3c.xn--b 1 aew.xn--p 1 ai/document/13608728.

35. Письмо Федеральной налоговой службы от 31.03.2016 № СА-4-7/5589 «О понятии «скриншот» («снимок экрана») и порядке его использования» [Электронный ресурс] // СПС «Гарант». — Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71284846/.

36. Приказ Министерства труда и социальной защиты РФ от 10.09.2019 № 611н «Об утверждении профессионального стандарта «Специалист по операциям с недвижимостью» [Электронный ресурс] // СПС «Гарант». — Режим доступа: https://base.garant.ru/73054922/.

37. Приказ Министерства труда и социальной защиты РФ от 24.07.2015 № 512н «Об утверждении профессионального стандарта «Специалист по финансовому мониторингу (в сфере противодействия легализации доходов, полученных преступным путем, и финансированию терроризма)» [Электронный ресурс] // СПС «Гарант». — Режим доступа: https://base.garant.ru/71165556/.

38. Приказ Министерства экономического развития Российской Федерации от 07.06.2017 № 278 «Об утверждении Административного регламента Федеральной службы государственной регистрации, кадастра и картографии по предоставлению государственной услуги по государственному кадастровому учету и (или) государственной регистрации прав на недвижимое имущество» [Электронный ресурс] // СПС «Гарант». — Режим доступа: https://www.garant.rU/products/ipo/prime/doc/71651130/?ysclid=m87cxhxpj80201762

39. Приказ Министерства юстиции РФ от 30.09.2020 № 229 «Об утверждении Порядка представления информации о нотариальном документе и формата ее размещения на документе с использованием машиночитаемой маркировки» [Электронный ресурс] // СПС «Гарант». — Режим доступа: https://base.garant.ru/74716450/.

40. Приказ ФСБ России от 19.07.2016 № 432 «Об утверждении Порядка представления организаторами распространения информации в информационно-телекоммуникационной сети «Интернет» в Федеральную службу безопасности Российской Федерации информации, необходимой для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет». Доступ из справ. правовой системы «КонсультантПлюс».

41. Приказ ФСО России от 07.09.2016 № 443 «Об утверждении Положения о российском государственном сегменте информационно-телекоммуникационной сети «Интернет». Доступ из справ. правовой системы «КонсультантПлюс».

42. Приказ МВД России от 29 авг. 2014 г. № 736 «Об утверждении Инструкции о порядке приема, регистрации и разрешении в территориальных органов Министерства внутренних дел Российской Федерации заявлений и сообщений о преступления, об административных правонарушениях». Доступ из справ. правовой системы «КонсультантПлюс».

43. Указание Генеральной прокуратуры, МВД, СК, ФСБ, ФТС России от 23.07.2020 "Об усилении прокурорского надзора и ведомственного контроля за органами, осуществляющими оперативно-розыскную деятельность, дознание и предварительное следствие по уголовным делам о преступлениях в сфере предпринимательской деятельности".

44. Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации: определение Конституционного Суда РФ от 25 янв. 2018 г. № 189-О. URL: http://doc.ksrf.ru/decision/KSRFDecision314926.pdf (дата обращения 19.03.2020).

45. Постановление Пленума Верховного Суда РФ от 15.11.2016 N 48 (ред. от 23.12.2025) "О практике применения судами законодательства,

регламентирующего особенности уголовной ответственности за преступления в сфере предпринимательской и иной экономической деятельности" Доступ из справ. правовой системы «КонсультантПлюс».

46. Обзор практики рассмотрения судами ходатайств о наложении ареста на имущество по основаниям, предусмотренным частью 1 статьи 115 Уголовно-процессуального кодекса Российской Федерации" (утв. Президиумом Верховного Суда РФ 27.03.2019).

47. Постановление Пленума Верховного Суда РФ от 30.11.2017 N 48 (ред. от 15.12.2022) "О судебной практике по делам о мошенничестве, присвоении и растрате".

II. Специальная литература

48. Абсатаров, Р. Р. Правовые проблемы изъятия электронных носителей информации и получения копий с них / Р. Р. Абсатаров // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. – 2023. – № 1(71). – С. 25-28. – EDN HEEXRC.

49. Агеев Н.В. Организация использования информационных технологий в расследовании / Гуманитарные, социально-экономические и общественные науки. Краснодар, 2022.

50. Андреева И.А., Васильченко А.А., Гаврилов Б.Я. Диссертационное исследование: технологии подготовки // Москва: Общество с ограниченной ответственностью "Проспект", 2025. – 360 с. – ISBN 978-5-392-43408-4. – DOI 10.31085/9785392310982-2020-360. – EDN CRIVRH.

51. Аносов А.В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, телекоммуникационных и высоких технологий: учеб. пособие: в 2 ч. / [А.В. Аносов и др.]. М.: Акад. управления МВД России, 2019. 208 с.

52. Антонов И.О., Шалимов А.Н. Актуальные проблемы расследования мошенничества с использованием компьютерной информации // Ученые записки казанского университета, Гуманитарные науки, 2015, том 157 кн.

53. Афанасьева С. И., Добровлянина О.В. Правовое регулирование производства следственных действий с использованием видео-конференц-связи по действующему упк рф // Ex jure. 2022. №4.

54. Бахтеев Д.В. Особенности фиксации и изъятия криминалистически значимой информации, размещенной в сети Интернет // Российский следователь. 2017. N 21. С. 10 - 13.

55. Белкин Р.С. Курс криминалистики: Криминалистические средства, приемы и рекомендации. В 3-х томах. Т. 3. - М.: Юристъ, 1997. - С. 68.

56. Белякова И.М., Добрина Т.Б. Проблема расследования экономических преступлений, совершенных с использованием информационных технологий и сетевого пространства // Эпоха науки №14 -Июнь 2018 г. Юридические науки.

57. Белоусов А.В., Смахтин Е.В. Криминалистическая модель искусственного интеллекта в системе уголовно-правовых наук // Известия ТулГУ. Экономические и юридические науки. 2024. №3.

58. Бертовский, Л. В. Высокотехнологичное право как элемент обеспечения национальной безопасности / Л. В. Бертовский // Правовая политика и правовая жизнь. – 2025. – № 1. – С. 202-207. – DOI 10.24412/1608-8794-2025-1-202-207. – EDN DTCFYB.

59. Бертовский, Л. В. Генеративный искусственный интеллект в контексте права интеллектуальной собственности и принципа ответственности: общие положения / Л. В. Бертовский, С. М. Курбатова // Наука и образование: опыт, проблемы, перспективы развития: Материалы международной научно-практической конференции, Красноярск, 16–18 апреля 2024 года. – Красноярск: Красноярский государственный аграрный университет, 2024. – С. 112-115. – EDN COSFXO.

60. Бертовский, Л. В. О некоторых проблемах цифрового судопроизводства / Л. В. Бертовский // Актуальные проблемы борьбы с преступностью: вопросы теории и практики: Материалы XXVII международной научно-практической конференции. В 2-х частях, Красноярск, 04–05 апреля 2024 года. – Красноярск: Сибирский юридический институт МВД РФ, 2024. – С. 155-157. – EDN SKWKNS.

61. Бертовский, Л. В. Основные направления развития криминалистической тактики / Л. В. Бертовский // Эксперт-криминалист. – 2025. – № 3. – С. 23-26. – DOI 10.18572/2072-442X-2025-3-23-26. – EDN ZCTXHI.

62. Бертовский, Л. В. Высокотехнологичное право как элемент обеспечения национальной безопасности / Л. В. Бертовский // Правовая политика и правовая жизнь. – 2025. – № 1. – С. 202-207. – DOI 10.24412/1608-8794-2025-1-202-207. – EDN DTCFYB.

63. Болвачев, М.А. Социальная сеть как объект криминалистического исследования / М.А. Болвачев // Известия Тульского государственного университета. Экономические и юридические науки. – 2020. – № 4. – С. 64-71

64. Бочкин Д.В. Способы совершения компьютерных преступлений и использование информационных технологий как способ совершения преступления // Сибирские уголовно-процессуальные и криминалистические чтения. Государство и право. Юридические науки. 2016. № 5(13). С. 40–46.

65. Булыжкин А.В., Бадиков Д.А. Некоторые особенности расследования преступлений, связанных с незаконным оборотом наркотических средств с использованием информационно-телекоммуникационных систем «Интернет»: практ. рекомендации. Орел: Орлов. юрид. ин-т МВД России им. В.В. Лукьянова, 2019. 31 с.

66. Бычков В.В., Вехов В.Б. Электронное следообразование преступной деятельности в сети Интернет//Расследование преступлений: проблемы и пути их решения. 2020. № 1 (27). С. 107.

67. Варданян, А. В. Преступления в сфере долевого строительства жилья и иных объектов недвижимости: проблемы законодательства и правоприменительной практики / А. В. Варданян // Всероссийский криминологический журнал. – 2022. – Т. 16, № 1. – С. 73-81. – DOI 10.17150/2500-4255.2022.16(1).73-81. – EDN EBJHDF.

68. Вазюлин С.А., Васюков В.Ф. Получение информации о соединениях между абонентами: специфика процедуры // Уголовный процесс. 2014. № 1. С. 10–21.

69. Варданян, А. В. Очная ставка и ее тактический потенциал для повышения результативности расследования преступлений в сфере земельных правоотношений / А. В. Варданян // Baikal Research Journal. – 2022. – Т. 13, № 1. – DOI 10.17150/2411-6262.2022.13(1).24. – EDN OMVOHK.

70. Варданян, А. В. Теоретические, методологические и гносеологические основы раскрытия, расследования преступлений в сфере внешнеэкономической деятельности / А. В. Варданян, К. А. Плясов. – Ростов-на-Дону: Ростовский юридический институт Министерства внутренних дел Российской Федерации, 2022. – 432 с. – ISBN 978-5-89288-470-9. – EDN VWWPZI.

71. Варданян, А. В. Специфика обстановки совершения преступлений в сфере земельных правоотношений и ее влияние на производство допросов подозреваемых, обвиняемых / А. В. Варданян, Г. А. Варданян // Вестник Дальневосточного юридического института МВД России. – 2022. – № 1(58). – С. 49-56. – EDN RPWDSL.

72. Варданян, А. В. Проблема систематизации цифровых методов оперативно-розыскной деятельности, используемых в борьбе с дистанционными хищениями, и их криминалистическое значение / А. В. Варданян // Юристъ-Правоведъ. – 2022. – № 2(101). – С. 7-13. – EDN TYUZMC.

73. Васюков В.Ф. Изъятие электронных носителей информации при производстве следственных действий: новеллы законодательства и проблемы

правоприменения // Вестник Томского государственного университета. Право. 2020. № 37. С. 32–39.

74. Васюков В.Ф., Булыжкин А.В. Изъятие электронных носителей информации при расследовании преступлений: нерешенные проблемы правового регулирования и правоприменения // Российский следователь. 2016. № 6. С. 3 - 8.

75. Вехов В.Б. Дорожка электронных следов: понятие и особенности судебного компьютерно-технического исследования // Уголовное производство: процессуальная теория и криминалистическая практика. Материалы VII Международной научно-практической конференции. Ответственные редакторы М.А. Михайлов, Т.В. Омельченко. 2019. С. 18–20.

76. Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств её обработки: монография. Волгоград: ВА МВД России, 2008. - 404 с.

77. Вехов В.Б. Получение компьютерной информации от организаторов ее распространения в сети Интернет как процессуальное действие // Расследование преступлений: проблемы и пути их решения. 2018. № 1 (19). С. 105–109.

78. Вехов В.Б., Баюш А.А. Правовой статус судебного эксперта и специалиста в процессуальном законодательстве российской федерации // Актуальные научные исследования в современном мире. 2019. № 10-2 (54). С. 98-101.

79. Вехов, В. Б. Дорожка электронных следов: понятие и особенности судебного компьютерно-технического исследования / В. Б. Вехов // Уголовное производство: процессуальная теория и криминалистическая практика : Материалы VII Международной научно-практической конференции, Алушта, 25–26 апреля 2019 года / Ответственные редакторы М.А. Михайлов, Т.В. Омельченко. – Алушта: Общество с ограниченной ответственностью «Издательство Типография «Ариал», 2019. – С. 18-20. – EDN EWPMFR.

80. Вехов, В. Б. Криминалистическое исследование цифровых отпечатков компьютерных устройств / В. Б. Вехов, А. Б. Смушкин //

Всероссийский криминологический журнал. – 2024. – Т. 18, № 4. – С. 390-397. – DOI 10.17150/2500-4255.2024.18(4).390-397. – EDN PCRWRC.

81. Вехов В. Б. Электронная криминалистика: понятие и система // Криминалистика: актуальные вопросы теории и практики : материалы междунар. науч.-практ. конференции. — Ростов н/Д : Изд-во Ростовский юридический институт МВД России, 2017. — С. 40-46.

82. Вехов, В. Б. Клавиатурный почерк, цифровые отпечатки и другие средства проверки цифрового алиби / В. Б. Вехов, А. Б. Смушкин // Вестник Саратовской государственной юридической академии. – 2025. – № 3(164). – С. 230-237. – DOI 10.24412/2227-7315-2025-3-230-237. – EDN GZZBHY.

83. Виноградова О. П. Криминалистические особенности исследования «цифрового алиби» // Известия Тульского государственного университета. Экономические и юридические науки. — 2023. — № 2. — С. 64-70.

84. Винокуров С. И. Криминалистическая характеристика преступления, ее содержание и роль в построении методики расследования конкретного вида преступлений // Методика расследования преступлений. Общие положения : материалы научно-практической конференции (г. Одесса, ноябрь 1976 г.). — Москва, 1976. — С. 101-104.

85. Волеводз, А. Г. Особенности международного взаимодействия при раскрытии и расследовании преступлений, совершаемых с использованием криптовалют / А. Г. Волеводз, К. К. Клевцов // Противодействие криптовалютным преступлениям в зарубежных странах. – Москва : ООО Издательский дом "Юрлитинформ", 2025. – С. 232-256. – EDN QSLBOG.

86. Волеводз, А. Г. Криптовалюта и цифровые финансовые активы как предмет и способ преступного посягательства / А. Г. Волеводз // Цифровое право : Учебник. – Москва : ООО Издательский дом "Юрлитинформ", 2024. – С. 589-599. – EDN NXOXMI.

87. Володченко В.С., Ланцова Д.С., Миронова Т.А. «Понятие и классификация информационных технологий» / «Достижения науки и образования», 2020.

88. Волчецкая, Т. С. Влияние цифровых технологий на современное развитие криминалистической науки / Т. С. Волчецкая // Современные технологии и подходы в юридической науке и образовании : Сборник материалов международного научно-практического форума, Калининград, 27–31 августа 2020 года. – Калининград: Балтийский федеральный университет имени Иммануила Канта, 2021. – С. 148-155. – EDN RCEYQW.

89. Волчецкая, Т. С. Развитие языка криминалистики в условиях цифровизации / Т. С. Волчецкая // Высокотехнологичное право: современные вызовы : Материалы IV Международной межвузовской научно-практической конференции, Москва-Красноярск, 17–20 февраля 2023 года. Том Часть 1. – Красноярск: Красноярский государственный аграрный университет, 2023. – С. 51-56. – EDN JFQPLE.

90. Волчецкая, Т. С. Особенности криминальных ситуаций при совершении мошенничества в сфере оборота недвижимости и следственных ситуаций в процессе его расследования / Т. С. Волчецкая, И. Е. Козырева, И. Ю. Панькина // Вестник Волгоградской академии МВД России. – 2023. – № 4(67). – С. 9-16. – DOI 10.25724/VAMVD.A187. – EDN MQSJRX.

91. Волчецкая Т. С. Криминалистическое моделирование в уголовном судопроизводстве : Учебно-методическое пособие / Т. С. Волчецкая, Е. В. Осипова. – Калининград : Балтийский федеральный университет имени Иммануила Канта, 2020. – 126 с.

92. Волчецкая Т.С. Роль, этапы и перспективы ситуационного подхода в современной криминалистике // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2016. № 4 (46). С. 9–11

93. Волчецкая Т.С. Криминалистическая ситуалогия: Монография. / Под ред. проф. Н.П. Яблокова. Москва; Калинингр. ун-т. - Калининград,1997.

94. Воронин М.И. Электронные доказательства в УПК: быть или не быть? // Lex russica. 2019. N 7. С. 74 - 84.

95. Гаврилин Ю.В., Победкин А.В. Использование информации, содержащейся на электронных носителях в уголовно-процессуальном доказывании: учеб. пособие / под ред. Ю.В. Гаврилина и А.В. Победкина. М., 2021. 140 с.

96. Гаврилин Ю.В., Балашова А.А. Совершенствование процессуального порядка собирания информации, содержащейся в сетевых информационных системах // Криминалистика: вчера, сегодня, завтра. 2020. № 1(13). С. 129–137.

97. Гаврилин Ю.В., Нуянзина С.В. Обеспечение законности при приеме, регистрации и разрешении сообщений о преступлениях, совершаемых с использованием информационно-телекоммуникационных технологий // Академическая мысль. 2020. № 4(13). С. 70–73.

98. Гармаев, Ю. П. Понятие преступлений, связанных с банкротствами юридических лиц, в криминалистическом аспекте / Ю. П. Гармаев, А. М. Федоров // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2025. – Т. 3, № 71. – С. 133-138. – EDN WEBQLG.

99. Гармаев, Ю. П. Прикладные криминалистические разработки в эпоху цифровизации / Ю. П. Гармаев // Криминалистические проблемы эффективности борьбы с преступностью и иными правонарушениями среди молодежи : Материалы международной научно-практической конференции, посвященной 100-летию Заслуженного деятеля науки Республики Башкортостан и Российской Федерации, доктора юридических наук, профессора Л.Л. Каневского, Уфа, 26 апреля 2024 года. – Уфа: Научно-исследовательский институт проблем правового государства, 2024. – С. 48-52. – EDN WTCXPI.

100. Гладких А.В. Социальные сети как новое средство совершения преступлений против собственности // Безопасность бизнеса. 2016. N 1. С. 33 - 36.

101. Головин А.Ю., Давыдов В.О. Криминалистическая категория «информационное обеспечение расследования преступлений» // Актуальные

проблемы криминалистики и судебной экспертизы. Материалы международной научно-практической конференции. 2020. С. 30–33.

102. Головин, А. Ю. Криминалистическая категория «информационное обеспечение расследования преступлений» / А. Ю. Головин, В. О. Давыдов // Актуальные проблемы криминалистики и судебной экспертизы : Материалы международной научно-практической конференции, Иркутск, 13–14 марта 2020 года. – Иркутск: Восточно-Сибирский институт Министерства внутренних дел Российской Федерации, 2020. – С. 30-33.

103. Головин А.Ю. Криминалистическая систематика: монография / под ред. Н.П. Яблокова. Москва: ЛексЭст, 2002. 335 с.

104. Головин, А. Ю. Технологии искусственного интеллекта в криминалистике: задачи, которые необходимо решить / А. Ю. Головин // Сибирские уголовно-процессуальные и криминалистические чтения. – 2024. – № 2(44). – С. 25-33. – DOI 10.17150/2411-6122.2024.2.25-33. – EDN WBXROE.

105. Грибунов, О. П. Криминалистическая модель лица, совершившего преступление: виды, особенности построения / О. П. Грибунов, Н. И. Валькирия // Государство и право. – 2024. – № 4. – С. 138-147. – DOI 10.31857/S1026945224040127. – EDN DWRDCR.

106. Григорьев А. Н. Использование в раскрытии и расследовании преступлений информации, полученной из открытых источников / А. Н. Григорьев // Наука и новация: современные проблемы теории и практики права: сборник материалов международной научно-практической конференции в рамках IV Международного Фестиваля науки, Москва, 20–21 февраля 2019 года. – Москва: Московский государственный областной университет, 2019. – С. 58-60.

107. Григорьев А. Н. Получение информации о времени при работе с электронными следами / А. Н. Григорьев, В. М. Мешков // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. – 2017. – № 2(48). – С. 10.

108. Григорьев А.Н., Бодылина Э.А., Информационно-телекоммуникационная сеть Интернет как среда и средство совершения преступлений // Материалы международной научно-практической конференции "Закон и правопорядок в третьем тысячелетии". Калининградский филиал Санкт-Петербургского университета МВД России. 2017. С. 72-73.

109. Григорьев А.Н., Мешков В.М. Получение информации о времени при работе с электронными следами / Григорьев А.Н., Мешков В.М. // Вестник калининградского филиала санкт-петербургского университета МВД России. - 2017. - № 2 (48). - С. 10

110. Давыдов, В. О. Цифровые следы в расследовании дистанционного мошенничества / В. О. Давыдов, И. В. Тишутина // Известия Тульского государственного университета. Экономические и юридические науки. – 2020. – № 3. – С. 20-27.

111. Давыдов, С. И. Вопросы оперативно-розыскного противодействия хищениям в агропромышленном комплексе / С. И. Давыдов // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. – 2024. – № 24. – С. 15-16. – EDN COCFZO.

112. Драпкин, Л. Я. Следственные ситуации: роль и значение в раскрытии и расследовании преступлений / Л. Я. Драпкин, Д. Л. Кокорин, И. Г. Пяткова. – Екатеринбург : Уральский юридический институт Министерства внутренних дел Российской Федерации, 2018. – 80 с. – ISBN 978-5-88437-558-1. – EDN UWUIMM.

113. Дремлюга Р.И., Крипакова А.В. Преступления в виртуальной реальности: миф или реальность? // Актуальные проблемы российского права. 2019. N 3. С. 161 - 169.

114. Дружинина А.А., Паулов П.А. Особенности реализации электронного судопроизводства в арбитражном процессе // Юридическая наука. М., 2021.

115. Дубоносов, Е. С. Оперативно-розыскное мероприятие "получение компьютерной информации": содержание и проблемы проведения / Е. С.

Дубоносов // Известия Тульского государственного университета. Экономические и юридические науки. – 2017. – № 2-2. – С. 24-30.

116. Журавлев, С.Ю. Знание о механизме экономических преступлений и его применение в процессе построения методик расследования / С.Ю. Журавлев. - Текст : непосредственный // Вестник научных школ Нижегородской академии МВД России : сборник статей / под науч. ред. М.П. Полякова. - Нижний Новгород : Нижегородская академия МВД России, 2011. - С. 251-264.

117. Журавлев, С.Ю. Механизм анализа криминальных схем в сфере экономики / С.Ю. Журавлев. - Текст : непосредственный // Экономическая безопасность России: политические ориентиры, законодательные приоритеты, практика обеспечения : Вестник Нижегородской академии МВД России. - 2006. - № 6. - С. 242-246.

118. Зуев С. В. Развитие информационных технологий в уголовном судопроизводстве: моногр. М. : Юрлитинформ, 2018. 248 с.

119. Ильин, И.В. Противодействие финансовой преступности (международный аспект) / И.В. Ильин, С.Л. Нудель. - Текст : непосредственный // Юридическая наука и практика : Вестник Нижегородской академии МВД России. - 2018. - № 4. - С.225-230.

120. Ишин А.М. Информационное обеспечение предварительного расследования преступлений: некоторые современные аспекты // Вестник Балтийского федерального университета им. И. Канта. Серия: Гуманитарные и общественные науки. Калининград, 2016.

121. Ищенко, Е.П. Виртуальный криминал: монография. – Москва: Юрлитинформ, 2011. – 208 с.; переиздание – 2013 г.

122. Касенова М.Б. Идентификация лиц в Интернете и киберпространство социальных сетей // Юрист. 2014. N 6. С. 32 - 36.

123. Ким Д.В., Брызгалов Г.Е. О некоторых проблемах предварительного расследования хищений денежных средств граждан с использованием

вредоносных компьютерных программ // Известия АлтГУ. Юридические науки. 2018 №3 (101).

124. Кириллов, М.А. Уклонение от уплаты налогов как угроза экономической безопасности государства / М.А. Кириллов, А.Р. Смирнов. - Текст : непосредственный // Вестник Российского университета кооперации. - 2021. - № 2. - С.131-135.

125. Клевцов К.К., Васюков В.Ф. Получение электронной информации по уголовным делам в рамках международного сотрудничества // Вестник Санкт-Петербургского университета. Право. 2021. Т. 12. № 1. С. 36–51.

126. Князьков, А. С. Проблемы тактики производства иных уголовно-процессуальных действий / А. С. Князьков // Материалы криминалистических чтений: Сборник материалов, Барнаул, 20–21 ноября 2025 года. – Барнаул: Барнаульский юридический институт МВД РФ, 2025. – С. 42-44.

127. Колычева А.Н., Васюков В.Ф. Расследование преступлений с использованием компьютерной информации из сети Интернет: учеб. пособие. М.: Проспект, 2022. 200 с.

128. Комарова Е.А. и Гундерич Г.А. Внедрение информационных технологий в уголовное судопроизводство. / Право и государство: теория и практика. Королев, 2020.

129. Кузнецов А.А., Муленков Д.В., Пропастин С.В., Соколов А.Б. Тактика следственных действий, направленных на отыскание, обнаружение, изъятие и исследование электронных носителей и информации на них: учеб. пособие. Омск: Омск. акад. МВД России, 2015. 116 с

130. Коняхин В.П., Асланян Р.Г. Информация как предмет и средство совершения преступлений в сфере экономической деятельности // Российский следователь. 2016. N 8. С. 24 - 27.

131. Криминалистика : учебник / Т. В. Аверьянова, Е. Р. Россинская, Р. С. Белкин, Ю. Г. Корухов. - 4-е изд., перераб. и доп. - Москва : Норма : Инфра-М, 2020. - 928 с.

132. Криминалистика в 5 Т. Том 5. Методика расследования преступлений : Учебник / Н. П. Яблоков, А. А. Беляков, И. В. Александров [и др.]. – 1-е изд. – Москва : Издательство Юрайт, 2020. – 242 с.

133. Литова В.А. «Сущность понятия "технология" на современном этапе» / Ученые записки. Электронный научный журнал Курского государственного университета, 2019

134. Майлис Н. П. Использование информационных ресурсов при производстве судебных экспертиз / Н. П. Майлис // Вестник экономической безопасности. – 2021. – № 3. – С. 166–169.

135. Макарейко, Н.В. Превентивный потенциал государственного принуждения в сфере обеспечения экономической безопасности / Н.В. Макарейко. - Текст : непосредственный // Юридическая наука и практика : Вестник Нижегородской академии МВД России. - 2017.- № 3. -С.219-223.

136. Макарейко, Н.В. Проблемы обеспечения экономической безопасности в условиях новых угроз / Н.В. Макарейко. - Текст : непосредственный // Юридическая наука и практика : Вестник Нижегородской академии МВД России. - 2021. - № 1. - С. 130-135.

137. Макаренко, И. А. Преступные нарушения законодательства об участии в долевом строительстве жилья и иных объектов недвижимости: уголовно-правовые и криминалистические аспекты / И. А. Макаренко, С. А. Григорян // Сибирские уголовно-процессуальные и криминалистические чтения. – 2021. – № 1(31). – С. 71-80. – EDN OECZNN.

138. Макаренко, И. А. Современное состояние и проблемы развития понятийного аппарата учения о предмете криминалистики / И. А. Макаренко, А. А. Эксархопуло // Сибирские уголовно-процессуальные и криминалистические чтения. – 2024. – № 4(46). – С. 64-74. – DOI 10.17150/2411-6122.2024.4.64-74. – EDN HZLFJQ

139. Макаренко, И. А. Сущность и правовые формы поисковой деятельности следователя / И. А. Макаренко, А. А. Эксархопуло // Философия права. – 2024. – № 4(111). – С. 146-153. – EDN LOESHV.

140. Макаренко, И. А. Способы разрешения конфликта при производстве вербальных следственных действий с участием обвиняемого / И. А. Макаренко // Вклад Л. Я. Драпкина в криминалистическую науку, Екатеринбург, 01 ноября 2019 года / Ответственный редактор: Д. В. Бахтеев. – Екатеринбург: Федеральное государственное бюджетное образовательное учреждение высшего образования "Уральский государственный юридический университет", 2019. – С. 189-197. – EDN UJFKWY.

141. Макаров Д.И., Шевченко О.И. «Цифровые технологии в банковской сфере» / Международный научный журнал «Символ науки» # 12-1-1, Уфа, 2023

142. Малыхина, Н. И. Цифровые следы как объект криминалистического исследования / Н. И. Малыхина // Современные технологии и подходы в юридической науке и образовании : Сборник материалов международного научно-практического форума, Калининград, 27–31 августа 2020 года. – Калининград: Балтийский федеральный университет имени Иммануила Канта, 2021. – С. 200-205.

143. Манукян А.Р. Экономические преступления в условиях цифровизации // Проблемы экономики и юридической практики. 2020. №1.

144. Маркова Т.В. Щербатых Д.А. Философия социальных сетей // Интерактивная наука. – 2018. DOI 10.21661/r-470385

145. Маханек, А.Б. Проблемы обеспечения прав участников уголовного судопроизводства при осмотре электронных носителей информации / А. Б. Маханек // Закон и правопорядок в Третьем тысячелетии: IX Балтийский юридический форум, материалы международной научно-практической конференции, Калининград, 12 декабря 2020 года. – Калининград: Калининградский филиал Санкт-Петербургского университета МВД России, 2021. – С. 31-33. – EDN BQWFQS.

146. Машукова М.В. Проблемы развития электронного гражданского судопроизводства в Российской Федерации // Актуальные проблемы гражданского судопроизводства: материалы межвузовской научно-практической конференции. Краснодар, 2017.

147. Мещеряков В. А. Криминалистические особенности получения компьютерной информации с цифровых носителей при производстве отдельных следственных действий / В. А. Мещеряков, О. Ю. Цурлуй // Эксперт-криминалист. – 2020. – № 2. – С. 15–17.

148. Мещеряков В.А. Следы цифрового века // Вопросы экспертной практики. 2019. № S1. С. 426.

149. Мещеряков В.А. Копирование информации с компьютерных носителей при производстве следственных действий / В. А. Мещеряков, О.Ю. Цурлуй // Цифровой след как объект судебной экспертизы : Материалы Международной научно-практической конференции, Москва, 17 января 2020 года. – Москва: РГ-Пресс, 2021. – С. 128-132.

150. Мещеряков В. А. Криминалистика в цифровой век / В. А. Мещеряков // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения) : Сборник статей Международной научно-практической конференции, Москва, 18 мая 2018 года. – Москва: Академия управления Министерства внутренних дел Российской Федерации, 2018. – С. 180-185.

151. Мещеряков В. А. Особенности использования специальных знаний в расследовании преступлений, связанных с применением информационных и телекоммуникационных технологий / В. А. Мещеряков // Воронежские криминалистические чтения. – 2017. – № 19. – С. 163-167.

152. Мещеряков В. А. Особенности специальных знаний, используемых в цифровой криминалистике / В. А. Мещеряков // Известия Тульского государственного университета. Экономические и юридические науки. – 2013. – № 4–2. – С. 88.

153. Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический анализ. Воронеж: Воронеж. гос. ун-т, 2001. 255 с.

154. Мещеряков В. А. Специальные знания в расследовании преступлений в сфере использования информационных и телекоммуникационных технологий / В. А. Мещеряков // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. – 2016. – № 1. – С. 11-15.

155. Мещеряков, В. А. Формирование дополнительных компетенций экспертов криминалистических экспертиз в сфере исследования информационных систем и компьютерных устройств / В. А. Мещеряков, Ю. М. Баркалов // Вестник Воронежского института МВД России. – 2020. – № 1. – С. 183-188.

156. Мещеряков, В. А. Цифровизация уголовного судопроизводства: продолжение / В. А. Мещеряков, О. Ю. Цурлуй // Теория и практика расследования преступлений : Материалы XI Международной научно-практической конференции, Краснодар, 13 апреля 2023 года. – Краснодар: Краснодарский университет МВД России, 2023. – С. 476-479. – EDN TVLNOR.

157. Мещеряков, В. А. Современное представление о механизме следообразования в современной информационной инфраструктуре / В. А. Мещеряков, О. Ю. Цурлуй // Информатизация и информационная безопасность правоохранительных органов : сборник трудов Международной научно-практической конференции, Москва, 30 июня 2023 года. – Москва: Академия управления МВД России, 2023. – С. 166-169. – EDN VKSBNA.

158. Микаева А.С. Проблемы правового регулирования в сети Интернет и их причины / Микаева А.С. //"Актуальные проблемы российского права". - 2016. - N 9. - С.45.

159. Модогоев, А. А. Организация и криминалистическая методика расследования экономических преступлений / А. А. Модогоев, С. И. Цветков. - Москва : Академия МВД СССР, 1990. - 86 с. - Текст : непосредственный.

160. Овчинский, В. С. Об угрозах квантовых компьютерных вычислений / В. С. Овчинский // Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции : Сборник материалов I Всероссийской научно-практической конференции, Москва, 27 января 2021 года. – Москва: Федеральное государственное казенное образовательное учреждение высшего образования "Университет прокуратуры Российской Федерации", 2021. – С. 54-60.

161. Орлова Т.В., Бушуев В.В. Формирование и развитие профессиональных компетенций судебного эксперта в области криминалистического исследования документов и портретной экспертизы // Вестник Московского университета МВД России. 2023. №2.

162. Осипенко, А.Л. Применение технологий искусственного интеллекта в юридической науке / А. Л. Осипенко // Общество и право. – 2024. – № 4(90). – С. 6-14. – EDN DBBAZV.

163. Осипенко, А.Л. Участие граждан в противодействии преступности в сфере информационных технологий / А. Л. Осипенко // Вестник Краснодарского университета МВД России. – 2025. – № 2(68). – С. 6-15. – EDN LZGTGL.

164. Пастухов П.С. О необходимости развития компьютерной криминалистики / под ред. О.А. Кузнецовой, В.Г. Голубцова, Г.Я. Борисевич, Л.В. Боровых, Ю.В. Васильевой, С.Г. Михайлова, С.Б. Полякова, А.С. Телегина, Т.В. Шершень // Пермский юридический альманах. Ежегодный научный журнал. 2018. N 1. С. 479 - 488.

165. Петров А.С. Перспективы применения информационных технологий в уголовном судопроизводстве // Вестник магистратуры. Йошкар- Ола, 2022.

166. Плахота К.С. Использование видео-конференц связи при расследовании преступлений. Вестник Краснодарского университета МВД России, Краснодар, 2021. С. 94-96.

167. Подольный, Н. А. Специальные знания при выявлении и расследовании киберпреступлений / Н. А. Подольный // Проблемы противодействия киберпреступности : Материалы III Международной научно-

практической конференции, Москва, 04 июня 2025 года. – Москва: Московская академия Следственного комитета РФ им. А.Я. Сухарева, 2025. – С. 95-101.

168. Подольный, Н. А. Системно-деятельностный подход в криминалистической методике расследования преступлений / Н. А. Подольный // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2025. – Т. 70, № 2. – С. 176-182.

169. Полстовалов, О. В. Обратная сторона цифровизации уголовного правосудия: новые вызовы для криминалистики и правоприменительной практики / О. В. Полстовалов // Современные технологии и подходы в юридической науке и образовании : Сборник материалов международного научно-практического форума, Калининград, 27–31 августа 2020 года. – Калининград: Балтийский федеральный университет имени Иммануила Канта, 2021. – С. 247-254.

170. Россинская Е.Р. Теория информационно-компьютерного обеспечения криминалистической деятельности. Монография. М, 2022. С 111.

171. Россинская, Е. Р. Тренды развития криминалистики в условиях цифровой трансформации современной преступности / Е. Р. Россинская // Союз криминалистов и криминологов. – 2025. – № 1. – С. 162-173

172. Россинская Е.Р., Рядовский И.А. Концепция цифровых следов в криминалистике // Аубакировские чтения: материалы Международной научно-практической конференции (19 февраля 2019 г.). Алматы, 2019. С. 6–8.

173. Россинская, Е. Р. Учение о цифровизации судебно-экспертной деятельности и проблемы судебно-экспертной дидактики / Е. Р. Россинская // Правовое государство: теория и практика. – 2020. – № 4–1(62). – С. 88–101.

174. Россинская Е.Р., Сааков Т.А. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров / Криминалистика: вчера, сегодня, завтра. Иркутск, 2020.

175. Россинская Е.Р., Савенков А.Н. Актуальные направления развития общей теории криминалистики сквозь призму современных технологий // Государство и право. 2024. N 10. С. 156-168.

176. Россинская Е.Р. К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 3-2. С. 109–117.

177. Россинский С.Б. Следственные действия: монография. М.: Норма, 2018. № 6. С. 118.

178. Савенков, А. Н. Актуальные направления развития общей теории криминалистики сквозь призму современных технологий / А. Н. Савенков, Е. Р. Россинская // Государство и право. – 2024. – № 10. – С. 156-168. – DOI 10.31857/S1026945224100145. – EDN CQBTPO.

179. Сариев Г.С. О возможностях использования цифровых технологий при расследовании преступлений // Вопросы российской юстиции. 2024. Вып. N 34. С. 402-411.

180. Саркисян Г.Г. Теоретическая и правовая основы оперативно-аналитической деятельности органов внутренних дел Российской Федерации: основные выводы и предложения // Труды Академии управления МВД России. 2023. №4 (68).

181. Садыгова Т. С. Социально-психологические функции социальных сетей // Вектор науки ТГУ. - 2012. - №3 (10). - С. 192-194.

182. Семикаленова А.И., Рядовский И.А. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики // Актуальные проблемы российского права. 2019. N 6. С. 178 - 185.

183. Семикаленова, А. И. Цифровые следы: неожиданные проблемы исследования / А. И. Семикаленова // Цифровой след как объект судебной экспертизы : Материалы Международной научно-практической конференции,

Москва, 17 января 2020 года. – Москва: РГ-Пресс, 2023. – С. 195-197. – EDN ONOGNK.

184. Смушкин, А. Б. Цифровизация криминалистической деятельности : + еПриложение: дополнительные материалы : учебное пособие для студентов магистратуры, обучающихся в юридических вузах, специалистов / А. Б. Смушкин. – Москва : Общество с ограниченной ответственностью "Издательство "КноРус", 2024. – 200 с. – ISBN 978-5-406-12879-4. – EDN ARTQFO.

185. Смушкин А. Б. Новые информационные компоненты в формировании электронных доказательств по уголовным делам (современная дорожка электронно-цифровых следов) // Сибирское юридическое обозрение. 2025. №3.

186. Сидорова И.Г. Способы позиционирования интернет-личности в социальной сети // Известия Волгоградского государственного педагогического университета. - 2013.

187. Скобелин С.Ю. Использование цифровых технологий при доказывании преступной деятельности // Российский следователь. 2019. N 3. С. 26 - 28.

188. Смагин П.Г. Эффективность использования отдельных видов информационных технологий при расследовании преступлений/ Вестник Воронежского института МВД России, 2021.

189. Смагин П.Г. Эффективность использования отдельных видов информационных технологий при расследовании преступлений/ Вестник Воронежского института МВД России, 2021.

190. Смагин П.Г. Использование моделей машинного обучения при расследовании преступлений в сфере информационных технологий / Вестник Воронежского института МВД России, 2024.

191. Смушкин А.Б. Виртуальные следы в криминалистике / А.Б. Смушкин // Законность. - 2012. - N 8. - С. 43.

192. Соколов, Ю. Н. Информационные технологии и оборот цифровых данных в криминалистике / Ю. Н. Соколов. – Екатеринбург : Федеральное государственное бюджетное образовательное учреждение высшего образования "Уральский государственный юридический университет", 2023. – 328 с. – ISBN 978-5-6049106-1-0. – EDN EGYKTJ.

193. Соловьев В.С. Преступность в социальных сетях интернета (криминологическое исследование по материалам судебной практики) /Соловьев В.С.// Криминологический журнал Байкальского государственного университета экономики и права. - 2016. - Т. 10, № 1. - С. 60–72.

194. Старичков М.В. Тактика осмотра и выемки носителей компьютерной информации // Вестник Восточно-Сибирского института Министерства внутренних дел России. 2012. № 2(61).

195. Старичков М.В. Получение информации о соединениях между абонентами и (или) абонентскими устройствами: тактика следственного действия // Юристъ-правовед. 2018. № 4(87). С. 199–203.

196. Стельмах В.Ю., Ефремова О.М., Васюков В.Ф. Производство следственных действий, направленных на получение и использование компьютерной информации: монография / под общ. ред. А.Г. Волеводза. М.: Проспект, 2021. 480 с.

197. Стельмах В.Ю. Получение информации о соединениях между абонентами и (или) абонентскими устройствами // LesRussia. 2017. № 3(124).

198. Степаненко, Д. А. Криминалистический анализ мошеннических действий, связанных с криптовалютой / Д. А. Степаненко, В. Е. Епифанцев // Право и правопорядок в фокусе научных исследований : Сборник научных трудов. – Хабаровск : Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Дальневосточный государственный университет путей сообщения", 2025. – С. 171-178.

199. Степанов В.В. «От информационных технологий к информационным онтологиям» / Ученые записки Крымского федерального университета имени В. И. Вернадского. Социология. Педагогика. Психология, 2012

200. Сергеев А.Б., Смахтин Е.В. Язык криминалистики и уголовного судопроизводства: теория и практика // Юридическая наука и правоохранительная практика. 2025. N 3 (73). С. 38-44.

201. Терентьева, Л. В. Понятие киберпространства и очерчивание его территориальных контуров / Л. В. Терентьева // Правовая информатика. – 2018. – № 4. – С. 66–71.

202. Толстухина, Т. В. Генезис судебно-экспертной деятельности / Т. В. Толстухина // Теоретические и практические основы функционирования межотраслевого института судебных экспертиз в рамках совершенствования деятельности Евразийского экономического союза : Сборник материалов ежегодной международной конференции, Тула, 15 ноября 2023 года. Том Выпуск X. – Тула: Тульский государственный университет, 2023. – С. 9-14. – EDN OKEAYM.

203. Трегубов С.Н. Основы уголовной техники, научно-технические приемы расследования преступлений. Москва: ЛексЭст, 2002. 336 с.

204. Ткачев А.В. Исследование компьютерной информации в криминалистике // Эксперт-криминалист. 2012. N 4. С. 5 - 8.

205. Урсул А. Д. Проблема информации в современной науке /А. Д. Урсул . - 1975

206. Холопова Е.Н. Ситуационная экспертиза: понятие, значение и возможности исследования // Ситуационный подход в юридической науке и практике: современные возможности и перспективы развития: Материалы Международной научно-практической конференции, посвященной 15-летию научной школы криминалистической ситуалогии БФУ им. И. Канта. 2017. С. 232–239.

207. Цимбал В.Н., Цимбал Н.Г. Использование информации социальных сетей Интернет в ходе предварительного расследования // Теория и практика общественного развития. 2013. Вып. 10. С. 425–427.

208. Чиненов Е.В. Правовые, психологические и организационно-тактические основы взаимодействия следователя с участниками расследования преступлений в сфере экономики, совершаемых на железнодорожном транспорте и объектах транспортной инфраструктуры // Юристъ-Правоведъ. 2023. № 1 (104). С. 178-187.

209. Чиненов Е.В. Теоретические основы методико-криминалистического обеспечения расследования преступлений в сфере экономики, совершаемых на железнодорожном транспорте // Проблемы правоохранительной деятельности. 2023. № 1. С. 44-49.

210. Шапиро Л.Г. Основные направления развития криминалистической методики в условиях цифровизации и глобализации преступности // Вестник Саратовской государственной юридической академии – 2021.

211. Шапиро Л. Г. Судебно-экономические экспертизы в борьбе с преступностью в сфере экономики [Текст] = Forensic economic expertises in combating criminality in the economic sphere : процессуальные и криминалистические проблемы / Л. Г. Шапиро // Вестник Саратовской государственной юридической академии. - 2016. - № 1. - С. 158-163. - Библиогр. в сносках. - полный текст статьи см. на сайте Научной электронной библиотеки https://elibrary.ru . - ISSN 2227-7315.

212. Шаталов А.С. Разработка методических основ расследования преступлений, совершаемых с помощью компьютерных и сетевых технологий: проблемы, перспективы и тенденции // Вестник Сибирского юридического института МВД России, 2018

213. Эксархопуло, А. А. Расследование преступлений, совершаемых на предприятиях топливно-энергетического комплекса : Учебное пособие для вузов / А. А. Эксархопуло, И. А. Макаренко, Р. И. Зайнуллин. – Москва : Общество с

ограниченной ответственностью "Издательство ЮРАЙТ", 2023. – 102 с. – (Высшее образование). – ISBN 978-5-534-15777-2. – EDN GIMXVU.

214. Яблоков Н.П. Криминалистика: природа, система, методологические основы. 2-е изд. М., 2009. С. 56.

215. Яблоков Н.П. Организованная преступная деятельность: теория и практика расследования. — М., 2014.

III. Авторефераты и диссертации

216. Агибалов В. Ю. Виртуальные следы в криминалистике и уголовном процессе : специальность 12.00.09 «Уголовный процесс» : автореф. дисс. … канд. юрид. наук / Агибалов Владимир Юрьевич. – Воронеж, 2010. – 24 с.

217. Александров, И.В. Основные проблемы организации и методики расследования современных экономических преступлений / И. В. Александров. - Текст : непосредственный // Современные проблемы организации следственной деятельности : материалы научно-практической конференции (Екатеринбург, 20 февраля 2014 года). - Екатеринбург : ООО УТ «Альфа Принт», 2014. - С. 90-97.

218. Атаманов Р.С. Основы методики расследования мошенничества в сети Интернет: автореф. дис. … канд. юрид. наук. М., 2012. 28 с.

219. Балашова А.А. Электронные носители информации и их использование в уголовно-процессуальном доказывании: дисс. ... канд. юрид. наук. М., 2020.

220. Бертовский Л.В. Проблемы теории и практики выявления и расследования преступного нарушения правил экономической деятельности : автореферат дис. ... доктора юридических наук : 12.00.09 / Моск. гос. юрид. акад.. — Москва, 2005. — 56 с.

221. Бертовский Л.В. Проблемы теории и практики выявления и расследования преступного нарушения правил экономической деятельности : автореферат дис. ... доктора юридических наук : 12.00.09 / Моск. гос. юрид. акад. - Москва, 2005. - 56 с.

222. Введенская, О.Ю. Особенности предварительного и первоначального этапов расследования незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий : специальность 51.40.00 : диссертация на соискание ученой степени кандидата юридических наук / Введенская Ольга Юрьевна, 2022. – 201 с. – EDN BRBCGO.

223. Вехов В.Б. Криминалистическая характеристика и совершенствование практики расследования и предупреждения преступлений, совершаемых с использованием средств компьютерной техники: автореф. дис. ... канд. юрид. наук. Волгоград, 1995. С. 15.

224. Вехов, В.Б. Криминалистическая характеристика и совершенствование практики расследования и предупреждения преступлений, совершаемых с использованием средств компьютерной техники: автореф. дис. ... канд. юрид. наук. Волгоград, 1995. - 27 с.

225. Волчецкая Т. С. Ситуационное моделирование в расследовании преступлений: автореф. дис. …канд. юрид. наук. М.: МГУ им. М.В. Ломоносова, 1991. – 23 с.

226. Волчецкая Т.С. Криминалистическая ситуалогия: дисс. …д-ра юрид. наук. М.: МГУ им. М.В. Ломоносова, 1997. – 395 с.

227. Волчецкая Т.С. Ситуационное моделирование в расследовании преступлений: дисс. … канд. юрид. наук. М., 1991. – 173 с.

228. Волынский, А.Ф. О способах противодействия расследованию экономических преступлений / А.Ф. Волынский. - Текст : непосредственный // Известия ТулГУ. Экономические и юридические науки. - Тула: Изд-во ТулГУ, 2013. - С. 27-36.

229. Гаврилин, Ю.В. Расследование преступлений, посягающих на информационную безопасность в сфере экономики: теоретические, организационно-тактические и методические основы: специальность12.00.09 «Уголовный процесс; криминалистика; оперативно-розыскная деятельность»:

диссертация на соискание ученой степени доктора юридических наук / Гав-рилин Юрий Викторович. - Москва, 2009. - 404 с. - Текст : непосредственный.

230. Евсиков К.С. Использование информационно-коммуникационных технологий в судебно-бухгалтерской экспертизе в процессе расследования преступлений в экономической сфере: дисс. ... канд. юрид. наук. Тула, 2011.

231. Ефремова В.А. Организация расследования преступлений экономической направленности: диссертация ... кандидата юридических наук : 12.00.11 / Ефремова Елена Александровна; [Место защиты: Акад. упр. МВД РФ]. - Москва, 2014. - 229 с. + Прил.(с. 1-146 : ил.).

232. Журавлев С.Ю. Методологические основы совершенствования методики расследования преступлений в сфере экономики : автореферат дис. ... доктора юридических наук : 5.1.4. / Журавлев Сергей Юрьевич; [Место защиты: ФГКОУ ВО «Нижегородская академия Министерства внутренних дел

233. Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: автореф. дис. … канд. юрид. наук. М., 2019. 25 с.

234. Костомаров К.В. Первоначальный этап расследования преступлений, связанных с незаконным доступом к компьютерной информации банков: дис. ... канд. юрид. наук. Екатеринбург, 2012. 212 с.

235. Курганова И.В. Криминалистическое моделирование при расследовании преступлений в сфере экономики : автореферат дис. ... кандидата юридических наук : 12.00.09 / Курганова Ираида Васильевна; [Место защиты: Нижегор. акад. МВД России]. - Нижний Новгород, 2008. - 27 с.

236. Лыткин Н.Н. Использование компьютерно-технических следов в расследовании преступлений против собственности: автореф. дис. … канд. юрид. наук. М., 2007. 24 с.

237. Льянов М.М. Криминалистическое значение электронно-цифровых следов преступлений экстремистской и террористической направленности в сети «Интернет»: автореф. дис. ... канд. юрид. наук. Екатеринбург, 2025. 25 с.

238. Мазуров И.Е. Методика расследования хищений, совершенных с использованием интернет-технологий: дис. … канд. юрид. наук. Ростов н/Д, 2017. 188 с.

239. Медведева М.О., Наточий С.Ю., Сафонов Г.И. «Понятие информационных технологий и их значение при расследовании преступлений» / «Вестник Московского Университета МВД России», М., 2021

240. Медведева М.А. Уголовно-процессуальная форма информационных технологий: современное состояние и основные направления развития: дисс. ... канд. юрид. наук. М., 2018.

241. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. дис. ... д-ра юрид. наук. Воронеж, 2001. 33 с.

242. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: дис. … д-ра юрид. наук. Воронеж, 2001. 387 с.

243. Милашев В.А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ: дис. … канд. юрид. наук. М., 2004. 204 с.

244. Оконенко Р.И. "Электронные доказательства" и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации: дисс. ... канд. юрид. наук. М., 2016.

245. Поздеев И.А. Организация взаимодействия следователя со сведущими лицами в ходе расследования разрушений строительных объектов: автореф. дис. … канд. юрид. наук. Челябинск, 2011. 25 с.

246. Савина Л.А. Организация и тактика предварительной проверки сообщений об экономических преступлениях на железнодорожном транспорте: дис. ... канд. юрид. наук. М., 2005. 228 с.

247. Сергеев М.С. Правовое регулирование применения электронной информации и электронных носителей информации в уголовном судопроизводстве: дисс. ... канд. юрид. наук. Казань, 2018.

248. Светличный А.А. Криминалистическая терминология в теории и практике противодействия преступной деятельности: автореф. дис. ... канд. юрид. наук. Калининград, 2024. 53 с.

249. Тлиш А.Д. Проблемы методики расследования преступлений в сфере экономической деятельности, совершаемых с использованием компьютерных технологий и пластиковых карт : Дис. ... канд. юрид. наук : 12.00.09 : Краснодар, 2002 253 с.

250. Черкасов В.С. Правовое регулирование применения электронных средств в доказывании на досудебных стадиях уголовного процесса: дисс. ... канд. юрид. наук. Челябинск, 2022.

251. Шапиро Л.Г. Специальные знания в уголовном судопроизводстве и их использование при расследовании преступлений в сфере экономической деятельности: автореферат дис. ... доктора юридических наук: Краснодар, 2008.

IV. Иностранная литература

252. Tim O'Reilly What Is Web 2.0 Design Patterns and Business Models for the Next Generation of Software [Электронный ресурс] URL: https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=3

V. Интернет – ресурсы

253. Алимов С.Р. Совершенствование использования информационных технологий при расследовании преступлений в сфере экономики Преступления в сфере экономики: организация и методика расследования – тема научной статьи по праву читайте бесплатно текст научно-исследовательской работы в электронной библиотеке КиберЛенинкаhttps://cyberleninka.ru/article/n/sovershenstvovanie-ispolzovaniya-

informatsionnyh-tehnologiy-pri-rassledovanii-prestupleniy-v-sfere-ekonomiki (дата обращения 23.11.2024).

254. Бессонов А. А. О некоторых возможностях современной криминалистики в работе с электронными следами // Вестник Университета имени О.Е. Кутафина. 2019. №3 (55). URL: https://cyberleninka.ru/article/n/o-nekotoryh-vozmozhnostyah-sovremennoy-kriminalistiki-v-rabote-s-elektronnymi-sledami (дата обращения 15.04.2023).

255. Волынский А.Ф. Преступления в сфере экономики: организация и методика расследования https://cyberleninka.ru/article/n/prestupleniya-v-sfere-ekonomiki-organizatsiya-i-metodika-rassledovaniya (дата обращения 11.11.2023).

256. Окоменко Р.И. Электронные доказательства как новое направление совершенствования российского уголовно-процессуального права // КиберЛенинка https://cyberleninka.ru/article/n/elektronnye-dokazatelstva kak-novoe-napravlenie-sovershenstvovaniya-rossiyskogo-ugolovno-protsessualnogo-prava (дата обращения 17.02.2023).

257. Коварин Д.А. Выявление, раскрытие и расследование преступлений в сфере экономики https://cyberleninka.ru/article/n/vyyavlenie-raskrytie-i-rassledovanie-prestupleniy-v-sfere-ekonomiki (дата обращения 23.11.2024).

258. Кручинина А.В. О криминалистическом обеспечении расследования преступлений в сфере экономики https://cyberleninka.ru/article/n/o-kriminalisticheskom-obespechenii-rassledovaniya-prestupleniy-v-sfere-ekonomiki

259. Посельская Л.Н. Интеграционная функция криминалистики в расследовании преступлений при переходе экономики на цифровые технологии https://cyberleninka.ru/article/n/integratsionnaya-funktsiya-kriminalistiki-v-rassledovanii-prestupleniy-pri-perehode-ekonomiki-na-tsifrovye-tehnologii

260. Суров О.А. Актуальные вопросы расследования преступлений в сфере экономики https://cyberleninka.ru/article/n/aktualnye-voprosy-rassledovaniya-prestupleniy-v-sfere-ekonomiki

261. Шапиро Л.Г. Основные направления развития криминалистической методики в условиях цифровизации и глобализации преступности // Киберленинка https://cyberleninka.ru/article/n/osnovnye-napravleniya-razvitiya-kriminalisticheskoy-metodiki-v-usloviyah-tsifrovizatsii-i-globalizatsii-prestupnosti?ysclid=mh13t93gsy895893420.

VI. Эмпирические материалы

262. Уголовные дела из Архива Центрального районного суда г. Калининграда (2014 -2024 гг) экономической направленности.

263. Уголовные дела из Архива Ленинградского районного суда г. Калининграда (2014 -2024 гг) экономической направленности

264. Уголовные дела из Архива Московского районного суда г. Калининграда (2014 -2024 гг) экономической направленности.

265. Уголовные дела из Архива Химкинского Городского суда Московской Области (2014 -2024 гг) экономической направленности.

266. Уголовные дела из Архива Чертановского районного суда г. Москвы (2014 -2024 гг) экономической направленности.

267. Уголовные дела из Архива Пресненского районного суда г. Москвы (2014 -2024 гг) экономической направленности.

268. Уголовные дела из Архива Фрунзенского районного суда г. Санкт-Петербурга (2014 -2024 гг) экономической направленности.

269. Уголовные дела из Архива Красносельского районного суда г. Санкт-Петербурга (2014 -2024 гг) экономической направленности.

270. Уголовные дела из Архива Смольнинского районного суда г. Санкт-Петербурга (2014 -2024 гг) экономической направленности.

271. Уголовные дела из Архива Выборгского городского суда Ленинградской области (2014 -2024 гг) экономической направленности.

272. Уголовные дела из Архива Боровичского районного суда Ногородской области (2014 -2024 гг) экономической направленности.

273. Уголовные дела из Архива Северодвинского городского суда Архзангельской области (2014 -2024 гг) экономической направленности.

274. Уголовные дела из Архива Азовского городского суда Ростовской области (2014 -2024 гг) экономической направленности.

275. Уголовные дела из Архива Первомайского районного суда г. Краснодара (2014 -2024 гг) экономической направленности.

276. Материалы из практики работы Главного следственного управления ГУ МВД России по г. Москве за 2022–2024 гг.

277. Материалы из практики работы Западного межрегионального следственного управления на транспорте СК России за 2022–2024 гг.

278. Материалы из практики работы СУ СК РФ по Калининградской области за 2022–2024 гг.

279. Материалы из практики работы СУ УМВД России по Калининградской области за 2022–2024 гг.

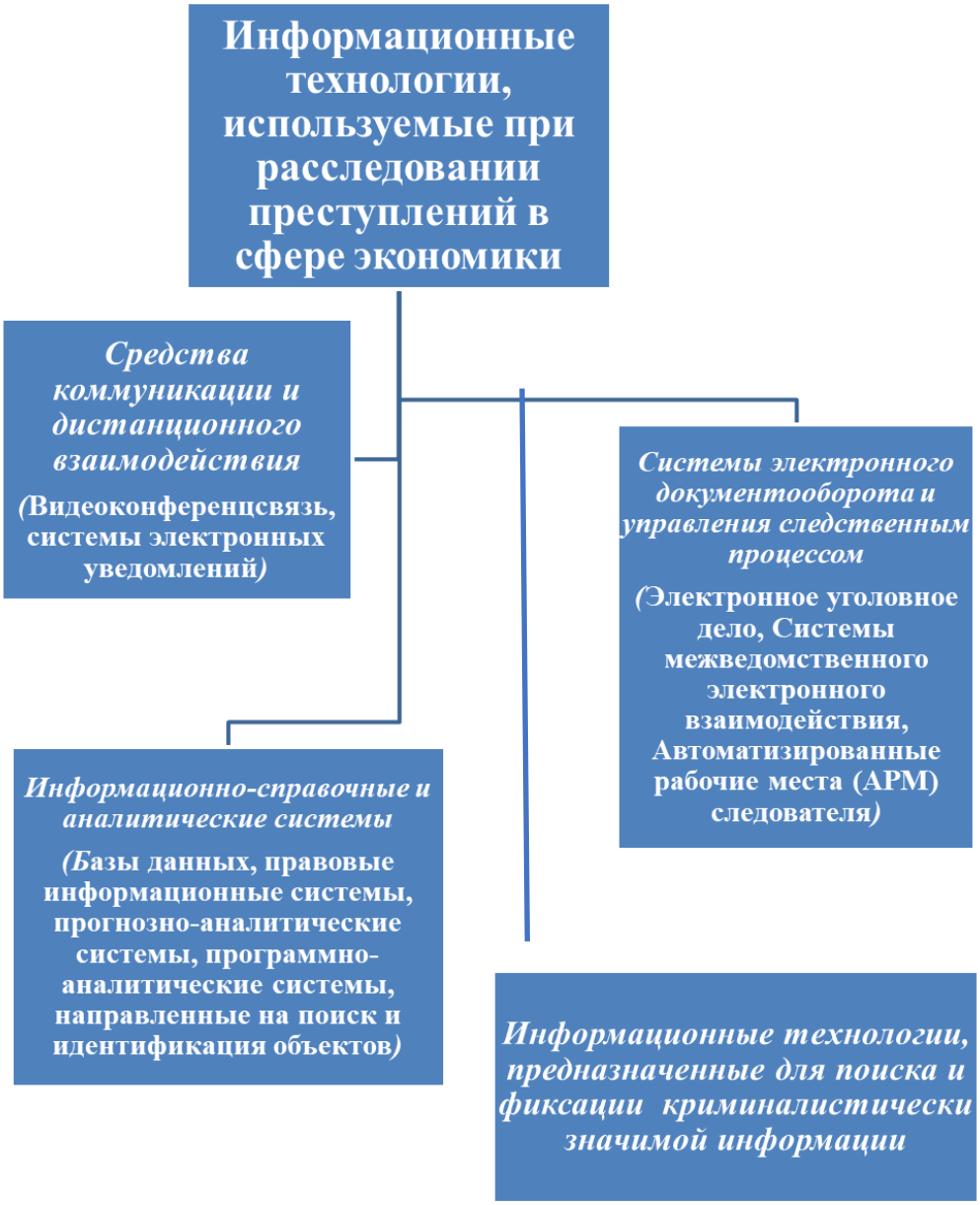
280. Материалы из практики работы СЧ по РОПД СУ УМВД России по Калининградской области за 2022–2024 гг.

281. Материалы из практики работы Северо-Западной оперативной таможни за 2022–2025 гг.

282. Материалы из практики работы отдела дознания Калининградской областной таможни за 2022–2025 гг.

Приложение №1

Иллюстрационная схема информационных технологий, используемых при расследовании преступлений в сфере экономики



Приложение №2

Иллюстрационная схема направлений использования информационных технологий в следственной практике

Приложение № 3

Аналитическая справка

по результатам интервьюирования следователей[1]

Каков Ваш стаж следственной работы?

В опросе приняли участие следователи с опытом работы:

- от 1 года до 3 лет – 12 человек (29%);
- от 3 до 5 лет –21 человек (48%).
- от 5 лет и более – 10 человек (23%).

Имеется ли в выданном Вам дипломе о высшем образовании сведения о пройденных курсах дисциплин «Информатика», «Основы ИКТ», либо иных, целью которых было изучение современных информационных технологий?

- *Да – 95%*
- *Нет – 5%*

Имеете ли Вы навыки изъятия базовых электронных носителей информации (мобильные телефоны, ноутбуки и иные)?

- *Да – 90%*
- *Нет – 10%*

Необходима ли Вам помощь специалиста при изъятии базовых электронных носителей информации (мобильные телефоны, ноутбуки и иные)?

[1] Всего проинтервьюировано 107 следователей, специализирующихся на расследовании преступлений в сфере экономики, в их числе 68 следователей подразделений МВД России и 39 следователей СК России, проходящих службу в следственных подразделениях Московской, Ленинградской, Мурманской, Сахалинской, Свердловской, Ростовской, Калининградской, Новгородской, Псковской областей, Краснодарского края, Республики Коми, г. Москвы и г. Санкт-Петербурга

- *Да – 5 %*
- *Нет – 95 %*

Как часто имеется необходимость в получении доказательственной информации с электронных носителей информации в ходе предварительного следствия?

- *Часто – 61 %*
- *Редко – 39 %*

Как часто имеется необходимость в получении доказательственной информации с электронных носителей информации в ходе предварительного следствия при расследовании преступлений в сфере экономики?

- *Часто – 85 %*
- *Редко – 15 %*

В ходе каких следственных действий чаще всего осуществляется изъятие электронных носителей информации?

- *Обыск – 90 %*
- *Выемка – 60 %*
- *Осмотр места происшествия – 15 %*

Как часто в ходе обысков/ выемок в ходе предварительного следствия имеется необходимость в изъятии электронных носителей информации?

- *Часто – 60 %*
- *Редко – 40 %*

Как часто в ходе обысков/ выемок в ходе предварительного следствия при расследовании преступлений в сфере экономики имеется необходимость в изъятии электронных носителей информации?

- *Часто – 88 %*
- *Редко – 12 %*

Какие электронные носители информации чаще подлежат изъятию в ходе следственных действий при расследовании преступлений в сфере экономики?

- *Персональные компьютеры, ноутбуки – 60 %*
- *Жесткие диски, USB-носители, съёмные жесткие диски, оптические диски – 55 %*
- *Мобильные телефоны – 85 %*
- *Сервера организаций, большие хранилища данных – 25 %*

Приложение № 4

Аналитическая справка

по результатам изучения материалов уголовных дел

В ходе проведения научного исследования всего было изучено 122 уголовных дела по преступлениям в сфере экономики находящихся в производстве следственных органов и рассмотренных судами Калининградской областей, г. Москвы, г. Санкт-Петербурга, Московской, Ленинградской, Новгородской, Архангельской областей, Краснодарского края, Ростовской области областях, а также рассмотренных судами первой и апелляционной инстанции г. Москвы, г. Санкт-Петербурга, Московской, Калининградской, Ленинградской, Новгородской, Архангельской областей, Краснодарского края, Ростовской области за период с 2012 по 2025 гг. на предмет особенностей изъятия электронных носителей информации при расследовании преступлений в сфере экономики.

Анализ протоколов обыска, выемки.

Выяснению подлежали следующие вопросы:

а) как часто проводятся следственные действия по изъятию электронных носителей информации при расследовании преступлений данной категории;

б) основания проведение изъятия электронного носителя информации;

в) как часто проводились следственные действия по копированию доказательственной информации с электронных носителей фигурантов на электронные носители сотрудников правоохранительных органов;

г) в каких ситуациях предпочтение отдается копированию информации с электронных носителей информации, а не их изъятию;

д) техническая возможность проведения копирования информации вместо изъятия электронных носителей при необходимости установления значимых обстоятельств уголовного дела;

е) тактическая целесообразность изъятия электронного носителя информации при отсутствии правовых оснований.

Анализ материалов уголовных дел позволил выявить следующие основные особенности и проблемы в контексте изъятия электронных носителей информации.

1. Закон строго регламентирует изъятие электронных носителей в экономических расследованиях (ст. 164.1 УПК). Изъятие допустимо только при возможности использования носителя для совершения преступления, у лица отсутствует право на его хранение, имеется судебное решение, разрешающее изъятие электронных носителей информации в ходе следственного действия, назначении экспертизы или невозможности копирования без потери/изменения данных. В иных ситуациях изъятие запрещено.

2. Из материалов изученных 73 % уголовных дел следует, что при расследовании преступлений рассматриваемой категории довольно часто применяется копирование информации с электронных носителей информации, вместо их изъятия. Однако такой процесс как копирование не позволяет в полной мере применить весь спектр инструментов, находящихся на «вооружении» специалиста, который возможно было бы применить в ходе экспертизы.

3. Следует констатировать, что нередким явлением является проведение обысков и выемок, набавленных на изъятие электронных носителей информации спустя значительное время после совершения преступления (45 % из числа изученных уголовных дел). Это часто приводит к тому, что интересующие файлы удалены с исследуемого носителя информации, что также препятствует ее копированию и требует применения специальных программ для их восстановления.

4. При попытке копирования информации с электронных носителей нередки случаи, когда владельцы электронных устройств отказываются предоставлять пароли и логины для доступа к электронной почте.

5. Анализ уголовных дел показал, что имелись случаи, когда следователи прибегали к способам фото и видео фиксации интересующей информации во время производства следственного действия (например переписки в мессенджере, копирование которой не представляется возможной) (25 %). Однако в этих случаях также не возможно установить удаленную информацию. Помимо этого, в данных случаях не представляется возможным исследовать «исходник» информации.

В большинстве случаев замена изъятия электронного носителя информации копированием приводила к отсутствию возможностей получения дополнительных доказательств, поскольку выявление удаленных, скрытых файлов, а также полное установление и копирование интересующих данных возможно только при полноценном исследовании носителя (осмотр с участием специалиста с применением аппаратно-программного комплекса или экспертиза).