УДК 343.98

И. А. Орешков

ПРОБЛЕМЫ ПОЛУЧЕНИЯ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В ЭЛЕКТРОННЫХ СООБЩЕНИЯХ, ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Балтийский федеральный университет им. И. Канта, Калининград, Россия
Поступила в редакцию 14.01.2025 г.
Принята к публикации 10.03.2025 г.
doi: 10.5922/vestnikhum-2025-2-3

Для цитирования: *Орешков И. А.* Проблемы получения доказательственной информации, содержащейся в электронных сообщениях, при расследовании преступлений // Вестник Балтийского федерального университета им. И. Канта. Сер.: Гуманитарные и общественные науки. 2025. №2. С. 34—44. doi: 10.5922/vestnikhum-2025-2-3.

Исследованы актуальные проблемы, возникающие в процессе расследования преступлений, связанных с получением информации, содержащейся в электронных сообщениях. В ходе исследования проведен анализ следственной практики, складывающейся при производстве следственного действия «выемка электронных сообщений в организациях, осуществляющих передачу данных по сетям связи». Выделены тактические и организационные проблемы, возникающие при проведении следственных действий, связанных с выемкой электронных сообщений в организациях, обеспечивающих их передачу посредством информационно-коммуникационной сети, проведен анализ ситуационной обусловленности проведения следственных действий, связанных с выемкой электронных сообщений, а также проблем, возникающих при их проведении. Цель научного исследования — разработка научно обоснованных рекомендаций по производству следственных действий, связанных с выемкой информации, содержащейся в электронных сообщениях. Материалами исследования послужили труды отечественных специалистов в области криминалистики, посвященные изучению проблем применения информационных технологий при расследовании преступлений; нормативные акты, регламентирующие процедуры выемки электронных сообщений и иных передаваемых по сетям электросвязи сообщений. В ходе исследования применялись методы анализа, систематизации и обобщения информации. В результате исследования выявлены недостатки процедуры проведения указанного следственного дела и отмечены преимущества. Даны методические рекомендации по тактике и методике проведения следственных действий, связанных с выемкой электронных и иных передаваемых по сетям электросвязи сообщений. Разработан алгоритм, содержащий комплекс следственных действий, направленный на установление наиболее полной и объективной совокупности электронных следов при расследовании преступлений различной направленности.

Ключевые слова: криминалистическое исследование, электронные сообщения, выемка сообщений, электронная почта, мессенджеры

При расследовании преступлений, в том числе в сфере экономики, можно отметить, что основополагающим способом получения электронных доказательств является изъятие электронных носителей и последующий анализ находящейся в них информации, в том числе и связанный с изучением электронных сообщений, находящихся в памяти указанных устройств или в облачных хранилищах, доступ к которым осуществляется посредством изъятого электронного носителя информации.

Вместе с тем при расследовании преступлений нередки случаи, когда необходимые электронные носители информации, в том числе содержащие электронные сообщения, переписки, не представляется возможным обнаружить в ходе следственных действий. Обычно подобные ситуации связаны с попытками воспрепятствовать расследованию через умышленное сокрытие или уничтожение носителей информации. Кроме того, другим фактором может быть то, что обнаруженные электронные устройства, к которым могут относиться мобильные телефоны (смартфоны), ноутбуки, настольные компьютеры и планшеты, зачастую оборудованы надежными средствами защиты. Без введения пароля доступ к таким устройствам может оказаться невозможным даже при проведении специальных исследований или экспертиз. Среди подобных электронных устройств можно выделить мобильные телефоны и ноутбуки, функционирующие на операционной системе iOS. В эту группу попадают не только известные продукты компании Apple, такие как iPhone или MacBook, но и аналогичные устройства от других производителей.

Указанные факторы обусловливают необходимость поиска иных средств и методов получения доказательственной информации посредством альтернативных источников [1, с. 151].

Прежде всего речь идет о возможностях доступа к СМС-сообщениям, электронным письмам, а также к переписке в социальных сетях и мессенджерах в организациях, обеспечивающих их передачу.

Рассматривая вопросы получения доказательственной информации, содержащейся в электронных сообщениях, необходимо первоначально определить содержание указанного понятия. В федеральном законе от 27.07.2006 №149-ФЗ (ред. от 08.08.2024) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.10.2024) под электронным сообщением понимается информация, переданная или полученная пользователем информационно-телекоммуникационной сети [9].

В криминалистике имеются различные точки зрения относительно трактовки определения электронных сообщений. Так, Ю.Н. Соколов считает, что это «электронные сообщения, создаваемые электронными устройствами с вложенными в них текстовыми, графическими, видео- и аудиофайлами [8, с. 272].

По мнению А.Н. Першина, «электронное сообщение отличается языковыми знаками компьютерного программирования и может нахо-

диться на машинных носителях постоянной или временной памяти или в электронно-волновой среде информационно-телекоммуникационных сетей» [6, с. 35].

С точки зрения Е.В. Никитиной и В.С. Раменской «электронное сообщение — сообщение, передаваемое по сетям электросвязи, которое может быть представлено как в форме текста, так и в ином виде (фото, видео)» [5, с. 26].

Резюмируя законодательные и научные формулировки понимания понятия электронных сообщений, можно отметить, что основными отличительными чертами электронных сообщений является факт их создания посредством электронного устройства и последующей передачи через информационно-телекоммуникационную сеть.

Таким образом, электронными сообщениями, например, нельзя признавать сообщения, передаваемые посредством радиосвязи, либо информацию, сохраненную на персональном компьютере в виде файла, но фактически не направленную посредством информационно-телекоммуникационной сети адресату, как и нельзя таковой считать информацию, сохраненную на электронных носителях, которые пересылаются посредством средств почтовой связи, курьерских организаций и т.д.

Альтернативным способом сбора цифровых доказательств в процессе расследования 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. Кроме того, к этой категории методов можно отнести отправку следственных запросов интернет-провайдерам и операторам связи. Эти действия подразумевают обращение к указанным провайдерам для получения доказательственной информации, которую они хранят на своих серверах. Таким образом, использование таких методов позволяет следственным органам эффективно запрашивать необходимую информацию и проводить более углубленное исследование цифровых следов, оставляемых пользователями в сети.

В настоящее время существуют методы получения такой информации на практике. Российские интернет-провайдеры и компании, предоставляющие сетевые услуги, в ответ на запросы правоохранительных органов передают данные, необходимые для ведения расследований. Это включает сведения о местоположении устройств, которые подключены к интернету по их IP-адресам.

В дополнение к этому в российских учреждениях, осуществляющих обмен сообщениями через сети электросвязи, в соответствии с судебным постановлением может быть осуществлена конфискация электронной почты и сообщений в социальных медиаплатформах. Этот механизм законодательно установлен в ч. 7 ст. 185 УПК РФ и был введен в действие в 2016 г. На практике он заключается в получении судебного решения в порядке, предусмотренном ст. 165 УПК РФ, и последующей выемке информации на основании этого решения в орга-

низациях, обеспечивающих передачу информации по сетям электросвязи, таких как почтовые сервисы и социальные сети. При этом в ходатайстве к суду о проведении выемки крайне важно указать на необходимость изъятия как существующих электронных сообщений на почтовом ящике в настоящее время, так и удаленных сообщений.

Как уже упоминалось, важно подать соответствующее ходатайство как можно раньше, так как удаленные данные хранятся на серверах компании — почтового сервиса лишь в течение полугода после их уничтожения.

Таким образом, принимая во внимание как время, затраченное на выявление преступления, так и период, необходимый для его расследования, можно утверждать, что электронная доказательственная информация в случае непринятия своевременных мер, направленных на ее изъятие, может быть безвозвратно утеряна. Ввиду этого нами был разработан специальный алгоритм, направленный на установление наибольшего количества электронных следов при расследовании преступлений различной направленности. Указанный алгоритм является универсальным применительно к расследованию как преступлений в сфере экономики, так и преступлений общеуголовной и коррупционной направленности. Данный алгоритм заключается в выполнении комплекса следственных и процессуальных действий, которые условно были нами разделены на три стадии. Первой стадией является сбор следственным путем информации о лицах (технических устройствах, абонентских номерах и т.д.), где может быть обнаружена криминалистически значимая информация [7, с. 126]. На второй стадии следователю необходимо спланировать и организовать проведение обысков или выемок. С целью изъятия электронных устройств, на которых может обнаружиться информация, представляющая интерес для следствия, проводятся следственные действия в местах проживания подозреваемых, а также на их рабочих местах или в местах выполнения служебных обязанностей. Третий этап включает в себя получение судебных постановлений, на основании которых осуществляется изъятие электронных сообщений и данных, хранящихся в облачных сервисах, в организациях, предоставляющих услуги передачи электронных сообщений.

При осуществлении предложенного алгоритма следственных и процессуальных действий возможно получить оптимальное количество доказательной информации как хранящейся на электронных носителях информации, так и передаваемой по сетям электросвязи, но которая ввиду противодействия расследованию со стороны заинтересованных лиц может быть удалена с технических средств, где ранее могла храниться.

Так, при расследовании уголовного дела по обвинению А. в совершении двух преступлений, предусмотренных ч. 4 ст. 159 Уголовного кодекса РФ, которое было возбуждено более чем через два года после совершения преступления, следователь в целях полноты сбора доказательственной информации и совокупности электронных следов, обратился с ходатайством в суд о производстве выемки электронных сооб-

щений, сохраненных и в том числе удаленных в отношении электронного почтового ящика n……..@mail.ru. После получения решения суда, разрешающего производство данного следственного действия, следователь с указанным решением суда прибыл в организацию, обеспечивающую передачу электронных сообщений — ООО «ВК», однако в ходе выемки выяснилось, что почтовый ящик пуст, что в том числе свидетельствует о том, что сообщения, которые там ранее находились, могли быть удалены, а срок хранения таких сообщений на серверах подобных организаций составляет 6 месяцев. Это означает, что даже при выполнении всех условий предложенного нами алгоритма следователь мог столкнуться с ситуацией, когда электронный почтовый ящик оказался пустым. Существует вероятность, что данная переписка была удалена на более раннем этапе — во время выявления и закрепления вышеуказанных обстоятельств в рамках оперативно-розыскных мероприятий либо на стадии проверки факта преступления в соответствии со ст. 144, 145 УПК РФ.

При обсуждении данного вопроса следует акцентировать внимание на том, что на самом деле органы, осуществляющие оперативно-розыскную деятельность, имеют право проводить оперативно-розыскные мероприятия, направленные на получение информации из электронных почтовых ящиков. Это возможно посредством проведения ОРМ «Наведение справок» или «Получение компьютерной информации» с предварительным получением разрешения суда. Такое тщательно спланированное проведение оперативно-розыскных мероприятий в случае необходимости длительной разработки преступной деятельности отдельных лиц или преступных групп может повысить качество дальнейшего доказывания вины конкретных лиц за совершение преступлений. Это также поможет предотвратить утрату существенно важных электронных улик, которые с трудом могут быть установлены в процессе расследования уголовного дела.

Кроме того, одной из ключевых рекомендаций является истребование в организациях, администрирующих сервисы электронной почты, социальные сети и мессенджеры, информации о регистрационных данных, указанных пользователем при создании аккаунта и электронного адреса, а также IP-адресов, с которых осуществлялась регистрация и активация при отправке сообщений. Наличие этих данных в совокупности имеет доказательное значение, подтверждающее факт общения конкретного лица.

Вместе с этим закрепленный в ч. 7 ст. 185 УПК РФ механизм изъятия электронных сообщений в организациях, обеспечивающих передачу сообщений по сетям электросвязи, в криминалистике вызывает много критики. В частности, ученые утверждают, что установленный в ч. 7 ст. 185 УПК РФ порядок производства выемки электронных сообщений противоречит порядку производства наложения ареста на почтово-телеграфные отправления, их осмотра и выемки, установленному ст. 185 УПК РФ, а не дополняет его. Указанные авторы свою научную позицию мотивируют тем, что сам механизм обмена электронными со-

общениями не предполагает возможность ареста указанных сообщений и их физическую выемку, поскольку они являются электронной информацией, также в результате следственного действия могут быть изготовлены лишь копии с серверов организаций, обеспечивающих передачу сообщений по сетям электросвязи [4, с. 29].

Указанный вопрос, на наш взгляд, является дискуссионным. Действительно, арест указанных сообщений в том понимании, который наиболее относится к почтовым отправлениям и связан с физической задержкой почтовых отправлений, их осмотром следователем в учреждении связи и последующим принятием решения о его копировании и дальнейшей отправке адресату, совсем не применим к сообщениям указанного вида.

Сама концепция отправки электронных сообщений заключается в мгновенном обмене сообщениями. Ввиду этого проработка моделей ареста, задержания и копирования указанной информации в аналогии с почтовыми отправлениями, на наш взгляд, является неприменимой к сообщениям данного вида.

Так, в социальных сетях или мессенджерах есть функции, предусматривающие оповещение о доставленном сообщении, а также о факте его прочтения. В связи с этим отсутствие оповещения о факте доставки и прочтении сообщения может спровоцировать у интересующего следствие лица подозрение о факте контроля этих сообщений со стороны правоохранительных органов. Кроме этого сама переписка может вестись непрерывно на протяжении определенного периода времени и в своей совокупности нести доказательственное значение, а какие-либо ее фрагменты, вырванные из контекста, не будут отражать полной картины событий, о которых идет речь.

Учитывая перечисленные обстоятельства, можно сделать вывод, что в ч. 7 ст. 185 УПК РФ не предусмотрено законодательное закрепление возможности ареста электронных сообщений и данных, пересылаемых через сети связи. В законе лишь указана возможность их осмотра и выемки.

Тем не менее в юридической науке существует мнение о том, что указанная норма права необоснованно включена в ст. 185 УПК РФ из-за отсутствия возможности произвести арест указанной корреспонденции, а также физическую выемку указанных сообщений ввиду их природы. Некоторые ученые в таком контексте предлагают выделить и законодательно регламентировать иные — новые — следственные действия, назвав их «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» [3, с. 251], «копирование и осмотр электронных сообщений и иных передаваемых по сетям электросвязи сообщений» [2, с. 479], «получение информации об электронных сообщениях, их копирование и осмотр» [5, с. 29].

Не разделяя вышеизложенные взгляды, но при этом не умаляя ценности представленных исследований, мы полагаем, что определение

следственного действия, связанного с изъятием электронных сообщений в процессе расследования уголовных дел непосредственно в организациях, обеспечивающих их передачу, регламентированное в законодательстве в настоящее время, является самым целесообразным и универсальным.

Рассматривая практику изъятия электронных сообщений или других данных, которые передаются по сетям связи, следует отметить, что фактически она сводится к двум основным действиям. Первое — получение решения суда о разрешении выемки электронных сообщений; второе — на основании полученного судебного решения выемка указанных сообщений, скопированных с серверов и сохраненных на материальный носитель в организации, обеспечивающей обмен указанными сообщениями.

Несмотря на то что вышеперечисленный способ получения доказательственной информации связан с выемкой носителя со скопированными сообщениями, мы считаем, что законодательно регулируемое понятие «выемка» является наиболее точным и широким — позволяющим на основании судебных решений проводить как выемку материальных носителей, содержащих уже скопированную с сервера информацию, так и выемку, связанную с самостоятельным просмотром имеющихся на сервере организации электронных сообщений с помощью привлеченного специалиста и проводить изъятие указанных сообщений с серверов организации с последующим ограничением доступа к ним на сервере со стороны каких-либо иных лиц, включая сотрудников указанной организации, обеспечивающей их передачу по сетям электросвязи. Таким образом, описанный выше способ получения доказательственной информации подразумевает под собой «перемещение», а не «копирование» информации.

Выемка электронных сообщений вышеописанным способом, а именно посредством их перемещения с сервера организации на другой электронный носитель информации, может проводиться, например, в тех следственных ситуациях, при которых требуется получить электронные сообщения и сведения о них в организациях, использующих собственные домены электронной почты. Во многих крупных организациях имеются собственные домены корпоративной почты, которая администрируется непосредственно самой организацией либо имеет собственный сервер.

Проводить выемку электронных сообщений с сервера указанных организаций посредством изъятия копий электронных сообщений, предварительно записанных на электронный носитель сотрудниками указанных организаций, во многих случаях будет тактически не верно. Зачастую руководители таких организаций не заинтересованы в предоставлении следователю полной и объективной картины электронной переписки корпоративной почты. Ввиду этого не исключен факт того, что следователю может быть предоставлена искаженная либо неполная информация. Эти обстоятельства подтверждают необходимость прове-

дения следственного действия — изъятия сведений, содержащихся в электронных сообщениях на почтовых ящиках таких организаций, описанным нами выше способом их «перемещения».

Правовым обоснованием для изъятия указанных сообщений является решение суда, поскольку данное следственное действие затрагивает конституционное право личности на тайну переписки. Как известно, ограничение конституционных прав граждан допустимо исключительно на основании судебного постановления. Мы разделяем научные мнения, согласно которым изъятие электронных сообщений невозможно без соответствующего решения суда.

Таким образом, мы считаем, что в целях выемки электронных сообщений, фактически сохраненных на корпоративных почтовых серверах посредством их «перемещения», следует в ходатайстве перед судом обосновать и мотивировать необходимость изъятия именно таким способом. Полагаем, что не нужно законодательно пытаться сузить предоставленную следственным органам возможность выбора тактики производства следственного действия, заключающегося в выемке информации, содержащейся в электронных сообщениях, сводя его только к копированию указанной информации с серверов организаций, осуществляющих их передачу посредством информационно-телекоммуникационной сети Интернет.

Существуют и другие проблемы, касающиеся изъятия электронных сообщений при расследовании преступлений. Например, сложность представляет получение данных об электронных переписках из зарубежных компаний, осуществляющих интернет-услуги, таких как Gmail, WhatsApp[1] и Telegram. Причин для затруднений несколько. Одна из них — ограниченное время хранения информации на серверах, что обусловлено законодательствами других стран и международными нормами. Кроме того, используется так называемое «сквозное шифрование», благодаря которому пересылаемые через чаты сообщения практически не сохраняются.

Дополнительные трудности возникают при обращении в компетентные органы зарубежных стран с запросами о правовой помощи в соответствии со ст. 453 УПК РФ. Эти препятствия связаны как с продолжительностью процесса подачи запросов и получения требуемой информации, так и с возможными рисками отказа в предоставлении таких данных. Согласно международным соглашениям, подписанным с Россией, иностранные власти могут отклонить такие запросы. Основания для отказа в исполнении запроса о правовой помощи, например, могут заключаться в том, что расследуемое деяние не является преступлением по уголовному закону иностранного государства или если запрашиваемые сведения могут угрожать его интересам.

Кроме того, наличие международного соглашения, подписанного между Российской Федерацией и данным государством, является одним из оснований для подачи запроса о правовой помощи в компетентные органы иностранного государства согласно ст. 453 УПК РФ.

---

[1] Приложение WhatsApp принадлежит компании *Meta*, которая признана в России экстремистской и запрещена.

Отсутствие заключенного Российской Федерацией и иностранным государством международно-правового договора об оказании взаимной правовой помощи по уголовным делам может быть причиной для отказа в удовлетворении запроса о правовой помощи, так как иностранное государство не будет иметь обязательств по его исполнению согласно действующему законодательству.

Мессенджеры имеют уникальные характеристики и установленные регламенты, которые определяют основания, условия и методы сотрудничества с органами правопорядка. Игнорирование этих норм может вызвать отказ зарубежного провайдера услуг в предоставлении требуемой информации, в том числе из-за ее отсутствия.

Тем не менее в случаях отыскания электронных доказательств в виде переписок в иностранных социальных сетях и мессенджерах, как ранее нами говорилось, следует своевременно планировать и проводить следственные действия по изъятию именно электронных носителей информации в целях установления, фиксации и в необходимых случаях восстановления сообщений, в том числе экспертным путем, которые могут иметь доказательственное значение для расследования уголовного дела.

Таким образом, получение доказательственной информации посредством проведения выемки электронных сообщений в учреждениях и организациях, обеспечивающих их передачу посредством сети Интернет имеет ряд отличительных особенностей, знание которых позволяет следователю более грамотно, рационально и эффективно планировать комплекс следственных действий как на первоначальном, так и на последующих этапах расследования преступлений. Знание указанных особенностей и соблюдение разработанных нами алгоритмов также способствуют принятию своевременных, всесторонних и объективных мер, направленных на установление, фиксацию и закрепление следов преступления (в том числе электронных следов, хранящихся на серверах организаций, обеспечивающих передачу электронных сообщений посредством информационно-телекоммуникационной сети), а также направленных на предотвращение возможной утраты этих следов.

Список литературы

1. *Волчецкая Т.С.* Влияние цифровых технологий на современное развитие криминалистической науки // Современные технологии и подходы в юридической науке и образовании : сб. матер. междунар. науч.-практ. форума. Калининград, 2021. С. 148—155.

2. *Гарипов Т.И.* Вопросы процессуальной регламентации копирования и осмотра электронных сообщений в уголовном судопроизводстве // Вестник Казанского юридического института МВД России. 2019. Т. 10, №4. С. 475—481. doi: 10.24420/KUI.2019.79.74.012.

3. *Зазулин А.И.* Правовые и методологические основы использования цифровой информации в доказывании по уголовному делу : дис. ... канд. юрид. наук. Екатеринбург, 2018.

4. *Мещеряков В.А.* «Виртуальные следы» под «Скальпелем Оккама» / Информационная безопасность регионов. Саратов, 2009. С. 28—33.

5. *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.

6. *Першин А.Н.* Электронный документ и электронное сообщение: понятие и особенности поиска в электронной среде // Научный вестник Омской академии МВД России. 2015 С. 34—38.

7. *Рамалданов Х.Х.* Понятие и сущность цифровизации доказательств и доказывания в уголовном судопроизводстве // Вестник Волгоградской академии МВД России. 2022. №1. С. 121—128.

8. *Соколов Ю.Н.* Информационные технологии и оборот цифровых данных в криминалистике: вопросы теории и практики. Екатеринбург, 2023.

9. *Об информации*, информационных технологиях и о защите информации : федер. закон от 27.07.2006 №149-ФЗ (ред. от 24.06.2025). Доступ из справ.-правовой системы «КонсультантПлюс».

Об авторе

Иван Андреевич Орешков — асп., Балтийский федеральный университет им. И. Канта, Калининград, Россия.

E-mail: vsmile777@mail.ru

I.A. Oreshkov

PROBLEMS OF OBTAINING EVIDENTIARY INFORMATION CONTAINED IN ELECTRONIC MESSAGES DURING CRIME INVESTIGATION

Immanuel Kant Baltic Federal University, Kaliningrad, Russia

Received 14 January 2025
Accepted 10 March 2025
doi: 10.5922/vestnikhum-2025-2-3

To cite this article: Oreshkov I.A. 2025, Problems of obtaining evidentiary information contained in electronic messages during crime investigation, *Vestnik of Immanuel Kant Baltic Federal University. Series: Humanities and social science*, №2. P. 34—44. doi: 10.5922/vestnikhum-2025-2-3.

The study examines current issues arising in the course of investigating crimes related to the acquisition of information contained in electronic communications. The research includes an analysis of investigative practices formed in the execution of the procedural action "seizure of electronic messages in organizations engaged in data transmission over communication networks." Tactical and organizational problems encountered during investigative actions involving the seizure of electronic messages in organizations that provide their transmission via information and communication networks are identified. An analysis is conducted on the situational conditionality of conducting investigative actions related to the seizure of electronic messages, as well as the challenges faced in this process. The objective of the scientific study is to develop scientifically grounded recommendations for conducting investigative actions related to the seizure of information contained in electronic messages. The study draws on the works of domestic experts in the field of forensics, focusing on the use of information technologies in crime investigations; normative legal acts regulating the procedures for seizing electronic messages and other communications transmitted over telecommunications networks. The research employed methods of analysis, systematization, and generalization of information. As a result of the study, deficiencies in the procedures for conducting the specified

investigative actions were identified, and advantages were noted. Methodological recommendations are provided regarding the tactics and methods of conducting investigative actions related to the seizure of electronic and other communications transmitted over telecommunications networks. An algorithm was developed containing a set of investigative measures aimed at establishing the most complete and objective body of electronic evidence in the investigation of various types of crimes.

Keywords: forensic investigation, electronic messages, message extraction, e-mail, messengers

The author

Ivan A. Oreshkov, PhD Student, Immanuel Kant Baltic Federal University, Kaliningrad, Russia.

E-mail: vsmile777@mail.ru