DOI 10.20310/2587-9340-2020-4-14-262-277
УДК 343.9
Шифр научной специальности 12.00.08

О НЕОБХОДИМОСТИ РАЗРАБОТКИ МЕТОДИКИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ОБРАЩЕНИЯ ЦИФРОВОЙ ИНФОРМАЦИИ

Э.М. Гильманов, Д.В. Кирпичников
ЧОУ ВО «Казанский инновационный университет им. В.Г. Тимирясова»
420111, Российская Федерация, г. Казань, ул. Московская, 42
ORCID: https://orcid.org/0000-0001-8181-9875, e-mail: elegys@mail.ru
ORCID: https://orcid.org/0000-0002-9958-512X, e-mail: danila667@outlook.com

Аннотация. Актуальность исследования обусловлена переходом процессов циркуляции информации о взаимодействии индивидов в информационно-телекоммуникационные устройства, их системы и сети, что обусловливает изменения в структуре преступности, детерминирует возникновение новых методов и способов совершения, запрещенных уголовным законом деяний. Сообразно изложенному, происходят изменения и в источниках отображения следовой информации о преступном событии, в качестве которых с все возрастающей частотой выступают информационно-телекоммуникационные устройства, их системы и сети. Названными обстоятельствами вызывается необходимость перехода от традиционных методик расследования преступлений в пользу тех приемов и способов, которые учитывают современный уровень технического развития, позволяют получать цифровую информацию и формировать на ее основе доказательства. Целью исследования является обоснование необходимости предложения новых методик расследования преступлений в сфере обращения цифровой информации. В ходе исследования на основе совокупности методов научного познания, в том числе абстрактно-логического, были проанализированы современные средства доказывания, исходя из чего сформулирован вывод о необходимости реформирования процессуального законодательства и скорейшей выработки новых средств и методов расследования преступлений. Обоснована необходимость активного использования новых видов специальной судебной экспертизы, а именно: информационно-технологической и информационно-технической, экспертизы электронно-цифровой подписи, процесса разработки и использования программного обеспечения, компьютерно-сетевой экспертизы, экспертизы обстоятельств создания и использования отдельных файлов, а также обсужден круг вопросов, решаемых посредством указанных экспертиз.

Ключевые слова: цифровая информация; методика расследования преступления; уголовное судопроизводство; следственные действия; тактические приемы; тактические комбинации; информационно-телекоммуникационные сети

В настоящее время ресурсами информационно-телекоммуникационных систем и сетей в значительной степени обеспечено функционирование и развитие большинства сфер деятельности человека. Кроме этого технический прогресс детерминирует перенос взаимодействия индивидов в цифровое пространство, сообразно чему и все материальные следы, отражающие их коммуникацию, для обеспечения их процессуальной фиксации требуют выявления, изъятия и исследования цифровой информации. Примечательно утверждение И.Р. Бегишева о том, что цифровая информация составляет основу в организации современных информационных соотношений, сформулированное ученым в 2011 г. [1, с. 47]. К аналогичным заключениям по результатам исследования пришли Е.В. Нечаева, Э.Ю. Латыпова и Э.М. Гильманов, указав на то, что укрепление национальной безопасности во многом зависит от развития информационного общества как в глобальном, так и национальном масштабе [2, с. 81].

Обратимся к ситуации, когда преступление совершается с использованием информационно-телекоммуникационных устройств (смартфона, компьютера, ноутбука и т. п.). В результате цифровизации социальных отношений при общении через различные гаджеты нередки случаи, когда потерпевший в ходе устной беседы не способен пояснить что-либо о своем контрагенте по общению ввиду того, что ограничен теми сведениями, которые последний изложил в своем профиле на странице сайта в сети Интернет. Таким образом, для получения полной и всесторонней информации об интересующем субъекте необходимо задействовать цифровую информацию, то есть сведения, сообщения и данные, обращающиеся в информационно-телекоммуникационных устройствах, их системах и сетях [3, с. 67]. В большинстве следственных ситуаций (данный тезис особенно очевиден при производстве по уголовным делам о преступлениях, предусмотренных статьями 137, 138 УК РФ, предусматривающих уголовную ответственность за нарушение неприкосновенности частной жизни и нарушение тайны переписки, телефонных, телеграфных и иных сообщений соответственно) производство традиционных допросов свидетелей и потерпевших либо направление запросов в адрес операторов связи не обеспечивает достижения криминалистически значимого результата [4]. То обстоятель-

ство, что основная часть сведений о преступлении отображается в информационно-телекоммуникационной сети [5], существенно снижает значимость показаний.

Полагаем, что потерпевший вполне в состоянии сообщить о том, как и при каких обстоятельствах было установлено взаимодействие, каким образом развивалась беседа, каковы были орфографические особенности электронных сообщений контрагента, однако маловероятно, что информация, полученная от гражданина, в какой-то степени окажется ценной для целей идентификации и обнаружения подозреваемого. Указанными обстоятельствами обусловливается необходимость изменения подходов к проверке сообщений и производству предварительного расследования в случае использования при совершении преступлений информационно-телекоммуникационных устройств, их систем и сетей. Представляется возможным констатировать, что при наличии в объективной стороне посягательства компьютерной информации образуется новая типовая криминалистическая характеристика отдельных видов преступлений, предопределяемая специфичным способом (предполагающим использование информационно-телекоммуникационных устройств, их систем и сетей), механизмом совершения преступления (использование средств защиты цифровой информации для сокрытия следов преступления), а также обстановкой совершения преступления (собственно сохранение основных следов в форме цифровой информации).

Широкое распространение цифровой коммуникации предопределяет появление новых способов совершения преступлений, механизмов создания и функционирования организованных групп, усложнение форм и методов преступной деятельности [6]. Указанная закономерность констатируется многими руководителями правоохранительных органов, в частности, совершенно справедливо утверждение Генерального прокурора Российской Федерации, высказанное в ходе выступления на расширенной коллегии Генеральной прокуратуры Российской Федерации, о том, что в 2019 г. продолжился рост преступлений, совершенных с использованием информационно-коммуникационных технологий[1]. Умножается количество мошенничеств с использованием

[1] Состоялось расширенное заседание коллегии, посвященное итогам работы органов прокуратуры за 2019 год и задачам по укреплению законности и правопорядка на 2020 год // Генеральная прокуратура Российской Федерации: официальный сайт. 2020. 17 марта. URL: http://www.genproc.gov.ru/smi/news/genproc/news-1809484/ (дата обращения: 20.03.2020).

электронных средств платежа [7; 8], в сфере компьютерной информации [9–11], фактов неправомерного доступа к компьютерной информации, в целом согласно актуальным данным в январе 2020 г. зарегистрировано 28,1 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 75,2 % больше, чем за аналогичный период прошлого года[2].

Основываясь на вышеизложенном, представляется возможным утверждать, что описанными обстоятельствами обусловлена необходимость коренного пересмотра подходов к организации деятельности по проверке сообщений о преступлениях и производстве предварительного расследования [12]. Типовые следственные ситуации, связанные с преступлениями различных видов, существенно изменились; информация, позволяющая обнаружить субъекта и пресечь его противоправную деятельность, в подавляющем большинстве случаев отображена в информационно-телекоммуникационных системах и сетях, которые являются единственными источниками, позволяющими формировать доказательства.

Думается, что предпочтительными являются те следственные и иные процессуальные действия, которые позволяют получать данные непосредственно от линии связи и от канала передачи информации, то есть коррелируют со средой распространения цифровой информации. Необходимо отметить, что сведениям о преступлении, представленным в форме цифровой последовательности сигналов, свойственны некоторые отличительные признаки, имеющие криминалистическое значение. Указанные свойства были выявлены И.Р. Бегишевым, который отметил, что цифровую информацию отличает простота в обработке информационно-телекоммуникационными устройствами, независимо от их назначения [12, с. 15-20]. Кроме этого, цифровая информация легко передается и обращается в информационно-телекоммуникационных устройствах, их системах и сетях; также эта информация легко создаваема и уничтожаема; более того, это и образует ее повышенное криминалистическое значение; информация может постоянно находиться в информационно-телекоммуникационном устройстве либо временно в каналах и сетях передачи информации, а также копируется неограниченное количество раз и без особых трудностей.

[2] Состояние преступности в России за январь 2020 года // Официальный сайт МВД России. URL: https://мвд.рф/reports/item/19655871 (дата обращения: 20.03.2020).

В затронутом контексте отметим, что в изложении о необходимости переработки тактических подходов к расследованию мы не рассматриваем ситуацию получения цифровой информации с устройства, поскольку, при его наличии, не составляет особых трудностей произвести выемку интересующей информации и направить ее на исследование с применением мобильного комплекса по сбору и анализу цифровых данных «UFED». Мы акцентируем рассуждения именно на тех ситуациях, когда криминалистически значимая цифровая информация концентрирована только в каналах и сетях передачи, то есть в ситуации, когда невозможно изъять и исследовать материальный носитель.

Думается, что более продуктивными, применительно к описанным ситуациям, являются такие следственные действия, как наложение ареста на почтово-телеграфные отправления, их осмотр и выемка в порядке статьи 185 УПК РФ (в части, касающейся случаев, когда имеются достаточные основания полагать, что сведения, имеющие значение для уголовного дела, содержатся в электронных сообщениях или иных сообщениях, передаваемых по каналам распространения цифровой информации); контроль и запись переговоров в порядке статьи 186 УПК РФ; получение информации о соединениях между абонентами и абонентскими устройствами в порядке статьи 186.1 УПК РФ. Обращаем внимание на то, что, согласно пункту 8 части 2 статьи 29 УПК РФ, в ходе досудебного производства по уголовному делу только суд правомочен принимать решения о наложении ареста на корреспонденцию, разрешении на ее осмотр и выемку в учреждениях связи; кроме этого, на основании пунктов 11, 12 части 2 статьи 29 УПК РФ, разрешение вопроса о производстве контроля и записи телефонных и иных переговоров, получении информации о соединениях между абонентами и абонентскими устройствами также относится к исключительной компетенции суда. Из изложенного следует, что для обеспечения оперативного принятия решения и фактического производства указанных следственных действий необходимо в кратчайшие сроки приискать информацию, достаточную для обоснования ходатайства, что предопределяет необходимость обеспечения эффективного оперативного сопровождения процесса расследования.

Только в ходе взаимодействия с оперативными сотрудниками возможно своевременное получение информации о содержании электронных сообщений субъектов, представляющих следственный интерес (для целей части 7 статьи 185 УПК РФ). При подготовке к получению судебного решения и фактическому производству следственного дей-

ствия, предусмотренного статьей 186 УПК РФ, оперативным сотрудникам поручается установление абонентских номеров связи, которыми пользуется изучаемое лицо, а также операторов связи, обслуживающих соединения абонента. Кроме этого, в ходе ОРД возможно получение иной информации, необходимой для подготовки и осуществления прослушивания телефонных переговоров, а именно: относительно личности лиц, в отношении которых планируется производство следственного действия; характеристик средств связи, которые используются для ведения переговоров; информации, необходимой для выбора формы прослушивания (автоматический режим, режим непосредственного прослушивания, сопровождающийся звукозаписью).

Названные рекомендации в равной степени актуальны для целей подготовки и осуществления следственного действия, предусмотренного статьей 186.1 УПК РФ. Кроме того, важно при решении вопроса о целесообразности производства следственных действий, предусмотренных статьями 185 и 186 УПК РФ, учитывать, что, согласно пункту 12 Постановления Правительства Российской Федерации № 538, в ходе взаимодействия с уполномоченными органами, осуществляющими ОРД, от оператора связи могут быть получены сведения об абонентах оператора связи, оказанных им услугах связи, в том числе информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео или иных сообщений пользователей услугами связи. Также имеет оперативное значение то обстоятельство, что вышепоименованная информация должна храниться оператором связи в течение 3 лет[3].

При этом необходимо обеспечивать удовлетворение предоставляемых результатов оперативно-розыскной деятельности требованиям межведомственной инструкции «О порядке предоставления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд». Так, согласно пункту 19 Инструкции, результаты ОРД, предоставляемые для подготовки и осуществления следственных действий, должны содержать сведения о фактах и обстоятельствах, позволяющих определить объем и последовательность проведения процессуальных действий, выбрать наиболее эффективную тактику их произ-

[3] Об утверждении правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность: постановление Правительства Российской Федерации от 27.09.2005 № 538 // СЗ РФ. 2005. №. 36. Ст. 3704.

водства, выработать оптимальную методику расследования по конкретному уголовному делу[4].

Исследуя возможности производства процессуальных действий для целей получения доказательственной информации, циркулирующей в информационно-телекоммуникационных устройствах, их системах и сетях, можно прийти к заключению, что перечень следственных действий, позволяющих выявлять, фиксировать, изымать и исследовать цифровую информацию, вполне обоснованно может быть дополнен [13, с. 298] и имеет перспективы к дальнейшему нормативному совершенствованию.

В рамках действующего уголовно-процессуального регулирования представляется мотивированным и целесообразным использование в доказывании по уголовным делам результатов оперативно-розыскной деятельности. Непосредственно УПК РФ содержит несколько абстрактные требования к подобным видам доказательств. Так, согласно статье 89 УПК РФ, в процессе доказывания запрещается использование результатов оперативно-розыскной деятельности, если они не отвечают требованиям, предъявляемым к доказательствам УПК РФ. Относительная конкретизация изложена в пункте 20 вышеуказанной Инструкции, которая предписывает, что результаты ОРД, представляемые для использования в доказывании по уголовным делам, должны позволять формировать доказательства, удовлетворяющие требованиям уголовно-процессуального законодательства, предъявляемые к доказательствам в целом, и к соответствующим видам доказательств: содержать сведения, имеющие значение для установления обстоятельств, подлежащих доказыванию при производстве по уголовному делу, указания на ОРМ, при проведении которых получены доказательства, а также данные, позволяющие проверить в ходе уголовного судопроизводства доказательства, сформированные на их основе [14, с. 293]. Можно предположить, что, используя в статье 89 УПК РФ абстракт-

[4] Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: приказ Министерства внутренних дел Российской Федерации, Министерства обороны Российской Федерации, Федеральной службы безопасности Российской Федерации, Федеральной службы охраны Российской Федерации, Федеральной таможенной службы, Службы внешней разведки Российской Федерации, Федеральной службы исполнения наказаний, Федеральной службы Российской Федерации по контролю за оборотом наркотиков, Следственного комитета Российской Федерации от 27.09.2013 № 776/703/509/507/1820/42/535/398/68. URL: https://rg.ru/gazeta/rg/2013/12/13.html (дата обращения: 22.03.2020).

ную терминологию, отсылающую к иным положениям процессуального закона, устанавливающим требования к доказательствам применительно к результатам оперативно-розыскной деятельности, законодатель предполагал – разъяснение соответствующих прав лицам, присутствующим при изъятии, привлечении к ОРМ общественных наблюдателей, соблюдение условий производства ОРМ. Кроме этого, с относительной долей условности на ОРМ также возможно распространить положения УПК РФ, регламентирующие общие правила производства следственных действий (статья 164 УПК РФ) и устанавливающие требования к форме и содержанию протокола (статья 166 УПК РФ). В данном контексте возможность применения общих положений УПК РФ применительно к ОРМ как никогда условны, однако, будучи достаточно абстрактными, названные нормы устанавливают обобщенные условия получения и фиксации доказательственной информации, при которых соблюдаются права и свободы участников, а также иных лиц, и порядок производства действия (мероприятия) [15, с. 96]. Распространение положений УПК РФ возможно в части разъяснения участвующим лицам их прав, обязанностей, ответственности, порядка производства ОРМ (не раскрывая при этом той части сведений, которая составляет государственную тайну), предупреждения о применении при проведении технических средств (за исключением тех, сведения о которых составляют государственную тайну). В любом случае, если тактическая обстановка позволяет, применение общих положений УПК РФ о следственном действии и протоколе однозначно гарантирует законность и обоснованность ОРМ. Доказательства, полученные таким образом, будут бесспорно легитимными, способными полагаться в основу обвинения, и использоваться для назначения и производства судебных экспертиз [16].

Для целей использования цифровой информации представляют особенный интерес такие оперативно-розыскные мероприятия, предусмотренные статьей 6 ФЗ № 144 «Об оперативно-розыскной деятельности», как контроль почтовых отправлений, телеграфных и иных сообщений, прослушивание телефонных переговоров, снятие информации с технических каналов связи, получение компьютерной информации.

В ходе планирования расследования и решения вопроса об избрании следственного действия или выдачи поручения о проведении ОРМ необходимо иметь в виду, что, согласно действующему законодательству, указанные оперативно-розыскные мероприятия могут проводиться только на основании судебного решения и только в отношении пре-

ступлений, относящихся к категории средней тяжести, тяжких и особо тяжких.

Нередко следственная ситуация тактически обусловливает большую эффективность выдачи поручения о производстве оперативно-розыскного мероприятия и дальнейшего использования его результатов в доказывании по уголовным делам. Выразим убеждение, что избрание подобной методики действительно удовлетворяет условиям тактического риска, позволяет оперативно получать значимую информацию, что обеспечивает полноту, всесторонность и своевременность расследования. Совершенно точно избрание подобной тактики необходимо на первоначальном этапе расследования, для целей оперативного обнаружения и фиксации следов преступления, требующих незамедлительного закрепления, изъятия и исследования. Поддержим мнение В.Н. Ельцова, справедливо отмечающего, что правоохранительные органы при расследовании правонарушений используют разнообразные средства и методы для достижения целей уголовного судопроизводства [17, с. 71], целью которых является не только назначение справедливого наказания, но и отказ от уголовного преследования невиновных.

Особую категорию цифровой информации составляют сведения об электронных финансовых операциях, осуществляемых с помощью информационно-телекоммуникационных устройств, их систем и сетей [18]. Дополнительную сложность образует то обстоятельство, что в отдельных случаях указанные сведения образуют банковскую или коммерческую тайну, сообразно этому, их выемка и осмотр возможны только на основании судебного решения. В любом случае, как справедливо отмечается в литературе, в настоящее время вопросы взаимодействия правоохранительных органов и отдельных коммерческих структур обладают недостаточной нормативной разработанностью, что усложняет процесс их взаимодействия [19, с. 152].

При разработке нормативно-правовых актов, регламентирующих подобное взаимодействие, необходимо ориентироваться на имеющуюся положительную практику информационного взаимодействия коммерческих организаций с отдельными органами безопасности. Так, согласно вышеуказанному Постановлению Правительства РФ № 538, оператором связи в адрес управлений отдельных органов безопасности по субъектам РФ, путем осуществления круглосуточного удаленного доступа, предоставляется информация, имеющаяся в базах данных оператора связи, что позволяет своевременно добывать оперативно значимую информацию, пресекать преступные деяния, фиксировать,

закреплять и исследовать материальные следы преступления, отраженные в виде цифровой информации, на основании чего строить дальнейшее доказывание по уголовным делам и выбирать методику расследования.

Взаимосвязанный комплекс особенных характеристик цифровой информации предопределяет необходимость производства по уголовным делам данной категории ряда нетипичных судебных экспертиз. Так, помимо традиционных криминалистической и дактилоскопической, следует назначать специальные судебные экспертизы – информационно-технологическую и информационно-техническую, а также, при появлении необходимости, экспертиз электронно-цифровой подписи, процесса разработки и использования программного обеспечения, компьютерно-сетевой экспертизы, экспертизы обстоятельств создания и использования файлов. Нельзя исключать возможность использования при совершении преступления и технологий искусственного интеллекта [20].

Предметное описание назначения и возможностей исследования названных экспертиз изложено в Методических рекомендациях по осуществлению прокурорского надзора. Согласно названному документу следует, что основанием для назначения информационно-технологической экспертизы является необходимость производства исследования и формулирования выводов по вопросам, требующим специальных познаний в области технологии информационных процессов. К таковым возможно отнести, в частности, объем вредных последствий, связанных с нарушением установленной технологии электронной обработки данных; причины нарушения установленной обработки компьютерной информации и т. п.

Информационно-техническая экспертиза назначается в том случае, когда в ходе следствия возникает необходимость в специальных исследованиях непосредственно технической части (отдельных узлов, блоков, периферийных устройств, оборудования, других носителей информации, обрабатываемых компьютерами, а также программных средств).

С учетом конкретных обстоятельств уголовного дела, на разрешение указанных разновидностей экспертных исследований могут быть поставлены иные вопросы, объем которых определяется следователем в зависимости от особенностей информационно-технологического или информационно-технического характера.

Так, по уголовным делам о неправомерном доступе к охраняемой законом компьютерной информации перед информационно-технологической экспертизой могут быть сформулированы вопросы о свойствах режима обработки данных и их охраны, применяемых в канале распространения информации технических средствах защиты цифровой информации, способах и средствах их нарушения.

В связи с вышеизложенным, полагаем, что назрела необходимость в создании современной методики расследования преступлений в сфере обращения цифровой информации, а также ее использования при совершении иных преступлений, где неправомерно используется цифровая информация.

Список литературы

1. *Бегишев И.Р.* Цифровая информация: понятие и сущность как предмета преступления по российскому уголовному праву // Академический юридический журнал. 2011. № 2 (44). С. 47-55.
2. *Нечаева Е.В., Латыпова Э.Ю., Гильманов Э.М.* Посягательства на цифровую информацию: современное состояние проблемы // Человек: преступление и наказание. 2019. Т. 27. № 1. С. 80-86.
3. *Бегишев И.Р., Бикеев И.И.* Преступления в сфере обращения цифровой информации. Казань: Изд-во «Познание» Казанского инновационного университета (Серия «Цифровая безопасность»), 2020. 300 с.
4. *Бурашникова Н.А.* К вопросу об оптимальной процессуальной форме судебного контроля за соблюдением права на свободу и личную неприкосновенность // Актуальные проблемы государства и права. 2019. Т. 3. № 11. С. 372-384. DOI 10.20310/2587-9340-2019-3-11-372-384.
5. *Latypova E.Y., Nechaeva E.V., Gilmanov E.M., Aleksandrova N.V.* Ingringements on Digital Information: Modern State of the Problem // SHS Web of Conferences. 2019. P. 10004. URL: https://doi.org/10.1051/shsconf/20196210004 (accessed: 17.03.2020).
6. *Латыпова Э.Ю.* Некоторые аспекты уголовной ответственности за деяния, посягающие на неприкосновенность частной жизни // Oeconomia et Jus. 2019. № 2. С. 35-45.
7. *Латыпова Э.Ю., Мусина Р.Р.* Некоторые проблемы мошенничества с помощью использования банковской карты с голосовым помощником // Информационные технологии в деятельности органов прокуратуры: сб. материалов 2 Всерос. науч.-практ. конф. / под общ. ред. Ф.Р. Хисамутдинова; сост. Ф.Н. Багаутдинов, А.А. Хайдаров. Казань: Казан. юрид. ин-т (филиал) Университета прокуратуры Российской Федерации, 2019. С. 109-112.
8. *Латыпова Э.Ю., Ключникова К.Е.* Проблемы уголовной ответственности за вымогательство с использованием виртуального шантажа // Информационные технологии в деятельности органов прокуратуры: сб. материалов 2 Всерос. науч.-практ. конф. / под общ. ред. Ф.Р. Хисамутдинова; сост. Ф.Н. Багаутдинов, А.А. Хайдаров. Казань: Казан. юрид. ин-т (филиал) Университета прокуратуры Российской Федерации, 2019. С. 113-115.

9. *Begishev I. R., Khisamova Z.I., Mazitova G.I.* Information infrastructure of safe computer attack // Helix. 2019. Vol. 9. № 5. P. 5639-5642. DOI: 10.29042/2019-5639-5642.
10. *Бегишев И.Р.* Безопасность критической информационной инфраструктуры Российской Федерации // Безопасность бизнеса. 2019. № 1. С. 27-32.
11. *Бегишев И.Р.* Некоторые механизмы совершенствования уголовного законодательства за совершение преступлений в сфере обращения цифровой информации // Information Security. 2017. № 6. С. 40-43.
12. *Бегишев И.Р.* Понятие и виды преступлений в сфере обращения цифровой информации: дис. … канд. юрид. наук. Казань, 2017. 204 с.
13. *Алпатов Д.С.* Криминалистическая характеристика новых составов совершения преступлений в сфере сотовой связи // Актуальные проблемы экономики и права. 2011. № 4. С. 296-299.
14. *Халиуллин А.И.* Место совершения преступления как признак состава преступления в сфере компьютерной информации // Актуальные проблемы экономики и права. 2012. № 1. С. 291-294.
15. *Немов В.А.* Демократичность или законность процедуры ограничения прав и свобод при проведении некоторых оперативно-розыскных мероприятий в Российской Федерации // Актуальные проблемы государства и права. 2018. Т. 2. № 5. С. 96-106. DOI: 10.20310/2587-9340-2018-2-5-96-106.
16. *Зажицкий В.И.* Результаты оперативно-розыскной деятельности в уголовном судопроизводстве. Теория и практика. М.: Изд-во Р. Асланова «Юридический центр Пресс», 2006. 590 с.
17. *Ельцов В.Н.* Процессуальные особенности задержания лица // Актуальные проблемы государства и права. 2018. Т. 2. № 6. С. 70-78. DOI: 10.20310/2587-9340-2018-2-6-70-78.
18. *Арюков А.К., Бегишев И.Р., Мальцев Н.А.* Некоторые аспекты информационной безопасности технологии блокчейн // Information Security. 2018. № 6. С. 18-19.
19. *Камко А.С.* Предупреждение мошенничества с использованием телекоммуникационного и компьютерного оборудования: дис. … канд. юрид. наук. Владивосток, 2020. 231 с.
20. *Бегишев И.Р., Латыпова Э.Ю., Кирпичников Д.В.* Искусственный интеллект как правовая категория: доктринальный подход к разработке дефиниции // Актуальные проблемы экономики и права. 2020. Т. 14. № 1. С. 79-91. DOI: http://dx.doi.org/10.21202/1993-047X.14.2020.1.79-91.

Поступила в редакцию 16.05.2020 г.
Поступила после рецензирования 11.06.2020 г.
Принята к публикации 26.06.2020 г.

Информация об авторах

Гильманов Эдуард Магасумьянович – старший преподаватель кафедры уголовного права и процесса. ЧОУ ВО «Казанский инновационный университет им. В.Г. Тимирясова», г. Казань, Российская Федерация.
ORCID: https://orcid.org/0000-0001-8181-9875, e-mail: elegys@mail.ru

Кирпичников Данила Владимирович – магистрант, кафедра уголовного права и процесса. ЧОУ ВО «Казанский инновационный университет им. В.Г. Тимирясова», г. Казань, Российская Федерация.
ORCID: https://orcid.org/0000-0002-9958-512X, e-mail: danila667@outlook.com

Для цитирования
Гильманов Э.М., Кирпичников Д.В. О необходимости разработки методики расследования преступлений в сфере обращения цифровой информации // Актуальные проблемы государства и права. 2020. Т. 4. № 14. С. 262-277. DOI 10.20310/2587-9340-2020-4-14-262-277

DOI 10.20310/2587-9340-2020-4-14-262-277

ON THE NEED TO DEVELOP A METHODOLOGY FOR INVESTIGATING CRIMES IN THE FIELD OF DIGITAL INFORMATION CIRCULATION

E.M. Gilmanov, D.V. Kirpichnikov
Kazan Innovative University named after V.G. Timiryasov
42 Moskovskaya St., Kazan 420111, Russian Federation
ORCID: https://orcid.org/0000-0001-8181-9875, e-mail: elegys@mail.ru
ORCID: https://orcid.org/0000-0002-9958-512X, e-mail: danila667@outlook.com

Abstract. The relevance of the study is due to the transition of the processes of circulating information about the interaction of individuals into information and telecommunication devices, its systems and networks, which causes changes in the structure of crime, determines the emergence of new methods and ways of committing acts prohibited by criminal law. In accordance with the above, changes are also taking place in the sources for displaying trace information about a criminal event, which are used by information and telecommunication devices, its systems and networks with increasing frequency. These circumstances necessitate the transition from traditional methods of crime investigation in favor of those techniques and methods that take into account the current level of technical development, allow us to receive digital information and generate evidence on its basis. The purpose of the work is to justify the need to offer new methods for investigating crimes in the field of digital information circulation. In the course of study based on a set of methods of scientific knowledge, including abstract and logical, modern means of evidence are analyzed, on the basis of which the conclusion is drawn about the need to reform the procedural legislation, and the early development of new means and methods of investigating crimes. We substantiate the need for the active use of new types of special forensic examination: information-technology, examination of digital signatures, the process of developing and using software, computer-network examination, circumstances examination

of the creation and use of individual files, and also discuss a range of issues addressed by these examinations.

Keywords: digital information; methods of crime investigation; criminal procedure; investigative actions; tactical techniques; tactical combinations; information and telecommunication networks

References

1. Begishev I.R. Tsifrovaya informatsiya: ponyatiye i sushchnost' kak predmeta prestupleniya po rossiyskomu ugolovnomu pravu [Digital information: notion and essence as a subject of crime under Russian criminal law]. *Akademicheskiy yuridicheskiy zhurnal – Academic Law Journal*, 2011, no. 2 (44), pp. 47-55. (In Russian).
2. Nechayeva E.V., Latypova E.Y., Gilmanov E.M. Posyagatel'stva na tsifrovuyu informatsiyu: sovremennoye sostoyaniye problemy [Attacks on digital information: the current state of the problem]. *Chelovek: prestupleniye i nakazaniye – Man: Crime and Punishment*, 2019, vol. 27, no. 1, pp. 80-86. (In Russian).
3. Begishev I.R., Bikeyev I.I. *Prestupleniya v sfere obrashcheniya tsifrovoy informatsii* [Crimes in the Sphere of Digital Information Circulation]. Kazan, Publishing House "Knowledge" of Kazan Innovation University ("Digital Security" Series), 2020, 300 p. (In Russian).
4. Burashnikova N.A. K voprosu ob optimal'noy protsessual'noy forme sudebnogo kontrolya za soblyudeniyem prava na svobodu i lichnuyu neprikosnovennost' [On the issue of the optimal procedural form of judicial control over the observance of the right to freedom and personal integrity]. *Aktual'nyye problemy gosudarstva i prava – Current Issues of the State and Law*, 2019, vol. 3, no. 11, pp. 372-384. DOI 10.20310/2587-9340-2019-3-11-372-384 (In Russian).
5. Latypova E.Y., Nechaeva E.V., Gilmanov E.M., Aleksandrova N.V. Ingringements on digital information: modern state of the problem. *SHS Web of Conferences*, 2019, p. 10004. Available at: https://doi.org/10.1051/shsconf/20196210004 (accessed 17.03.2020).
6. Latypova E.Y. Nekotoryye aspekty ugolovnoy otvetstvennosti za deyaniya, posyagayushchiye na neprikosnovennost' chastnoy zhizni [Some aspects of criminal liability for personal privacy infringement]. *Oeconomia et Jus*, 2019, no. 2, pp. 35-45. (In Russian).
7. Latypova E.Y., Musina R.R. Nekotoryye problemy moshennichestva s pomoshch'yu ispol'zovaniya bankovskoy karty s golosovym pomoshchnikom [Some fraud issues using a bank card with voice assistant]. *Sbornik materialov 2 Vserossiyskoy nauchno-prakticheskoy konferentsii «Informatsionnyye tekhnologii v deyatel'nosti organov prokuratury»* [Proceedings of 2nd All-Russian Research and Practice Conference "Information Technology in the Activities of Prosecutors"]. Kazan, The Kazan Law Institute (branch) of the Academy of General Prosecutor's Office, 2019, pp. 109-112. (In Russian).
8. Latypova E.Y., Klyuchnikova K.E. Problemy ugolovnoy otvetstvennosti za vymogatel'stvo s ispol'zovaniyem virtual'nogo shantazha [Problems of criminal liability for extortion using virtual blackmail]. *Sbornik materialov 2 Vserossiyskoy nauchno-prakticheskoy konferentsii «Informatsionnyye tekhnologii v deyatel'nosti organov prokuratury»* [Proceedings of 2nd All-Russian Research and Practice Conference "Information Technology in the Activities of Prosecutors"]. Kazan, The Kazan Law Institute

(branch) of the Academy of General Prosecutor's Office, 2019, pp. 113-115. (In Russian).
9. Begishev I. R., Khisamova Z.I., Mazitova G.I. Information infrastructure of safe computer attack. *Helix*, 2019, vol. 9, no. 5, pp. 5639-5642. DOI: 10.29042/2019-5639-5642.
10. Begishev I.R. Bezopasnost' kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii [Security of critical information infrastructure of the Russian federation]. *Bezopasnost' biznesa – Business Security*, 2019, no. 1, pp. 27-32. (In Russian).
11. Begishev I.R. Nekotoryye mekhanizmy sovershenstvovaniya ugolovnogo zakonodatel'stva za sovershenie prestupleniy v sfere obrashcheniya tsifrovoy informatsii [Some mechanisms for improving the criminal law for committing crimes in the field of the circulation of digital information]. *Information Security*, 2017, no. 6, pp. 40-43. (In Russian).
12. Begishev I.R. *Ponyatiye i vidy prestupleniy v sfere obrashcheniya tsifrovoy informatsii: dis. ... kand. yurid. nauk* [The Concept and Types of Crimes in the Field of Digital Information. Cand. jurid. sci. diss.]. Kazan, 2017, 204 p. (In Russian).
13. Alpatov D.S. Kriminalisticheskaya kharakteristika novykh sostavov sovershenia prestupleniy v sfere sotovoy svyazi [Criminalistical characteristic of new ways of committing crimes in the sphere of cellular communication]. *Aktual'nyye problemy ekonomiki i prava – Actual Problems of Economics and Law*, 2011, no. 4, pp. 296-299. (In Russian).
14. Khaliullin A.I. Mesto sovershenia prestupleniya kak priznak sostava prestupleniya v sfere komp'yuternoy informatsii [Place of crime as a sign of crime in the field of computer information]. *Aktual'nyye problemy ekonomiki i prava – Actual Problems of Economics and Law*, 2012, no. 1, pp. 291-294. (In Russian).
15. Nemov V.A. Demokratichnost' ili zakonnost' protsedury ogranicheniya prav i svobod pri provedenii nekotorykh operativno-rozysknykh meropriyatiy v Rossiyskoy Federatsii [Democracy or legality of the procedure of restriction of rights and freedoms when carrying out some special investigative activities in the Russian Federation]. *Aktual'nyye problemy gosudarstva i prava – Current Issues of the State and Law*, 2018, vol. 2, no. 5, pp. 96-106. DOI: 10.20310/2587-9340-2018-2-5-96-106. (In Russian).
16. Zazhitskiy V.I. *Rezul'taty operativno-rozysknoy deyatel'nosti v ugolovnom sudoproizvodstve. Teoriya i praktik*a [The Results of Operational and Investigative Activities in Criminal Proceedings: Theory and Practice]. Moscow, R. Aslanov Publishing House "Yuridichesky Center Press", 2006, 590 p. (In Russian).
17. Eltsov V.N. Protsessual'nyye osobennosti zaderzhaniya litsa [Procedural features of detention of a person]. *Aktual'nyye problemy gosudarstva i prava – Current Issues of the State and Law*, 2018, vol. 2, no. 6, pp. 70-78. DOI: 10.20310/2587-9340-2018-2-6-70-78. (In Russian).
18. Aryukov A.K., Begishev I.R., Maltsev N.A. Nekotoryye aspekty informatsionnoy bezopasnosti tekhnologii blokcheyn [Some aspects of information security blockchain technology]. *Information Security*, 2018, no. 6, pp. 18-19. (In Russian).
19. Kamko A.S. *Preduprezhdeniye moshennichestva s ispol'zovaniyem telekommunikatsionnogo i komp'yuternogo oborudovaniya: dis. ... kand. yurid. nauk* [Telecommunication and Computer Equipment Fraud Prevention. Cand. jurid. sci. diss.]. Vladivostok, 2020, 231 p. (In Russian).

20. Begishev I.R., Latypova E.Y., Kirpichnikov D.V. Iskusstvennyy intellekt kak pravovaya kategoriya: doktrinal'nyy podkhod k razrabotke definitsii [Artificial intelligence as a legal category: doctrinal approach to formulating a definition]. *Aktual'nyye problemy ekonomiki i prava – Actual Problems of Economics and Law*, 2020, vol. 14, no. 1, pp. 79-91. DOI: http://dx.doi.org/10.21202/1993-047X.14.2020.1.79-91. (In Russian).

Received 16 May 2020
Reviewed 11 June 2020
Accepted for press 26 June 2020

Information about the authors

Gilmanov Eduard Magasumyanovich – Senior Lecturer of Criminal Law and Procedure Department. Kazan Innovative University named after V.G. Timiryasov, Kazan, Russian Federation.
ORCID: https://orcid.org/0000-0001-8181-9875, e-mail: elegys@mail.ru
Kirpichnikov Danila Vladimirovich – Master's Degree Student, Criminal Law and Procedure Department. Kazan Innovative University named after V.G. Timiryasov, Kazan, Russian Federation.
ORCID: https://orcid.org/0000-0002-9958-512X, e-mail: danila667@outlook.com

For citation

Gilmanov E.M., Kirpichnikov D.V. O neobkhodimosti razrabotki metodiki rassledovaniya prestupleniy v sfere obrashcheniya tsifrovoy informatsii [On the need to develop a methodology for investigating crimes in the field of digital information circulation]. *Aktual'nye problemy gosudarstva i prava – Current Issues of the State and Law*, 2020, vol. 4, no. 14, pp. 262-277. DOI 10.20310/2587-9340-2020-4-14-262-277 (In Russian, Abstr. in Engl.)