DOI: 10.17803/1994-1471.2025.170.1.180-187

А. Б. Смушкин*

Криминалистическое исследование распределенной информации

Аннотация. В статье констатируется повышение значения новой формы информации — распределенной информации. Анализируются правовые события, вызывающие необходимость криминалистического исследования распределенной информации, а также наиболее часто совершаемые с использованием сервисов распределенной информации преступления. Излагаются основные правила функционирования систем распределенной информации. Обращается внимание на то, что наиболее часто в практике расследования возникает необходимость исследования именно файлообменных сетей, в частности такой их разновидности, как торренты. Рассматриваются основы функционирования файлообменных сетей. С учетом проведенного исследования предлагается авторская классификация файлообменных сетей. В работе определены основные криминалистически значимые задачи исследования файлообменных сетей. К ним отнесены: восстановление целого информационного объекта по частям; установление пользователя и его идентификаторов; доказывание осведомленности пользователя о содержании имеющихся у него информационных объектов; доказывание умысла на распространение; последовательно рассмотрены основы решения указанных задач. В ходе компаративистского исследования привлечения к ответственности провайдеров файлообменных сетей был сделан вывод, что в России, в отличие от многих зарубежных стран, практически отсутствует правовая база для привлечения к ответственности провайдера пиринговых сетей (но и в сетях последнего поколения у провайдера практически не остается контроля за контентом сети). Отмечаются недостаточные знания большинства следователей в рассматриваемой сфере. Представляется насущно необходимой организация периодических курсов повышения квалификации с рассмотрением новых технологий и основ их исследования.

Ключевые слова: криминалистическое исследование файлообменных сетей; цифровая криминалистика; торренты; трекеры; виртуальные следы; ответственность провайдера файлообменной сети; доказывание вины нарушителей; расследование; децентрализованные сети; пиринговые сети.

Для цитирования: *Смушкин А. Б.* Криминалистическое исследование распределенной информации // Актуальные проблемы российского права. — 2025. — Т. 20. — № 1. — С. 180–187. — DOI: 10.17803/1994-1471.2025.170.1.180-187.

Благодарности. Исследование выполнено за счет гранта Российского научного фонда № 24-28-00312, https://rscf.ru/project/24-28-00312/.

* *Смушкин Александр Борисович*, ведущий научный сотрудник проектного офиса научных программ и исследований Саратовской государственной юридической академии, доцент кафедры криминалистики Саратовской государственной юридической академии
Чернышевского ул., д. 104, г. Саратов, Российская Федерация, 410028
skif32@yandex.ru

Forensic Investigation of Distributed Information

Aleksandr B. Smushkin, Leading Researcher, Project Office of Scientific Programs and Research, Saratov State Law Academy, Associate Professor, Department of Criminalistics, Saratov State Law Academy, Saratov, Russian Federation
skif32@yandex.ru

Abstract. The paper notes the increasing importance of a new form of information–distributed information. The author analyzes legal events that necessitate forensic research of distributed information, as well as the most frequently committed crimes using distributed information services. The basic rules for the functioning of distributed information systems are defined. It is stated that most often in the practice of investigation there is a need to study file-sharing networks and their variety such as torrents. The basics of file-sharing networks are considered. Taking into account the conducted research, the author's classification of file-sharing networks is proposed. The paper defines the main forensically significant tasks of studying file-sharing networks. These include: restoration of the entire information object from parts; identification of the user and his identifiers; proof of the user's awareness of the content of the information objects in his possession; proof of intent to distribute; the principles of solving the above problems are considered sequentially. In the course of a comparative study of holding file-sharing network providers accountable, it was found that, unlike many foreign countries, in Russia there is virtually no legal basis for holding a peer-to-peer network provider accountable (but even in the latest generation of networks, the provider has virtually no control over the content of the network). It is noted that most investigators have insufficient knowledge in the area under consideration. It seems urgently necessary to organize periodic advanced training courses that cover new technologies and the principles of their research.

Keywords: forensic examination of file-sharing networks; digital forensics; torrents; trackers; virtual traces; liability of the provider of the file-sharing network; proving the guilt of violators; investigation; decentralized networks; peer-to-peer networks.
Cite as: Smushkin AB. Forensic Investigation of Distributed Information. *Aktual'nye problemy rossijskogo prava*. 2025;20(1):180-187. (In Russ.). DOI: 10.17803/1994-1471.2025.170.1.180-187.

Acknowledgements. The study was supported by the Russian Science Foundation, grant No. 24-28-00312, https://rscf.ru/project/24-28-00312/.

Четвертая информационная революция, повсеместная активизация и усложнение применяемых технических средств коммуникации, хранения и обработки информации, цифровизация всех сфер человеческой жизни приводят к возникновению новых концептов в информационной сфере и новых форм информации. Одной из таких форм является распределенная информация.

Наиболее часто необходимость в исследовании сервисов распределенной информации возникает при расследовании дистанционной незаконной торговли наркотиками (через маркетплейсы Даркнета), распространения экстремистской информации, использования мессенджеров, основанных на соответствующих технологиях, при организации и управлении не только экстремистским или террористическим, но любым иным преступным сообществом, распространении детской порнографии, нарушении авторских прав и т.д. М. Ф. Радайкин обоснованно отметил, что «файлообмен проблемным контентом будет оставаться до тех пор, пока не станет выгоднее и проще работать официально, нежели в серой или черной схеме»[1].

[1] *Радайкин М. Ф.* Правовое положение торрент-трекеров и их пользователей // Интеллектуальная собственность. Авторское право и смежные права. 2013. № 4. С. 50.

Системы и сервисы распределенной информации функционируют на основе следующих правил:

— единый информационный объект (включая композитные объекты типа дискографий, собраний сочинений, программных комплексов) дробится на множество элементов;

— как правило, в сети отсутствует единый центр и все ее пользователи равны;

— информационный объект скачивается и раздается параллельно несколькими потоками;

— полученные элементы информационного объекта, в свою очередь, попадают на раздачу у нового пользователя;

— чем больше в сети раздающих, тем выше скорость перекачки;

— в определенный момент в сети может не быть ни одного пользователя, обладающего полным информационным объектом;

— использование первоначальным владельцем полного файла VPN-сервисов и прокси-серверов существенно осложняет либо вообще делает невозможным его установление.

Видами использования распределенной информации можно считать:

— файлообменные пиринговые сети и торренты;

— системы распределенных вычислений;

— блокчейн;

— некоторые виды удаленного цифрового видеонаблюдения;

— некоторые мессенджеры типа «скайп».

Наиболее часто возникает необходимость исследования именно файлообменных сетей, в частности торрентов.

Е. А. Войниканис отмечает три основных принципа функционирования файлообменной сети:

— «взаимного использования ресурсов;

— децентрализации;

— самоорганизации»[2].

Первый принцип характеризуется предоставлением информации и компьютерных мощностей фактически в общее пользование. Имея много общего с распределенной базой данных, в пиринговой сети пользователь предоставляет доступ к части своего дискового пространства.

Принцип децентрализации означает отсутствие единых серверов, с которых происходит скачивание информации, неприменение клиент-серверной схемы. Отсутствие выраженного центра не дает возможности выявить конкретного злоумышленника или блокировать конкретный ресурс.

Принцип самоорганизации заключается в корреляции структуры конкретной файлообменной сети с количеством участников, количеством и характером операций в сети.

Принципиальная основа функционирования торрентов достаточно подробно описана Е. Ю. Бакировой и А. Л. Свинарем как сообщение присоединившимся к торренту пользователем своего адреса в сети и получение адресов передающих или скачивающих тот же файл пользователей: «Данные пользователи по частям скачивают друг у друга недостающие фрагменты определенного файла, получая на выходе совокупность всех частей этого файла, т.е. файл целиком»[3]. Таким образом, трекеры предоставляют только адреса пользователей, не участвуя в самом процессе обмена файлами, а пользователи соединяются напрямую в произвольных конфигурациях.

Активно используются технологии пиринговых (от англ. Peer-to-peer, p2p — равный к равному) файлообменных сетей в рамках Даркнета — теневого интернета — для ограничения доступа и анонимизации участников.

Классификация файлообменных сетей может производиться по различным основаниям. По типу организации сети можно выделить ча-

[2] *Войниканис Е. А.* Проблемы охраны результатов интеллектуальной деятельности в пиринговых сетях // Современное право. 2009. № 3. С. 106.

[3] *Бакирова Е. Ю.*, *Свинарь А. Л.* Защита авторских прав в сети Интернет на примере файлообменых сетей // Проблемы законодательного регулирования ресурсов и правового разрешения конфликтов с участием субъектов интернет-сообщества : материалы междунар. науч.-практ. конференции в рамках проекта «Российско-украинские криминалистические чтения на Слобожанщине», г. Белгород, 19 апреля 2013 г. / отв. ред. И. М. Комаров. Белгород : НИУ «БелГУ», 2013. С. 26.

стично децентрализованные сети (например, торренты с сервером, на котором размещаются адреса пользователей, владеющих информационными объектами), полностью децентрализованные (классические пиринговые сети и сети friend-to-friend). По степени открытости можно выделить: полностью открытые сети (допускающие скачивание без регистрации); требующие регистрацию, но не ограничивающие ее; сети с ограниченной регистрацией (либо требующие приглашения участника сети, либо сети с ограниченной пропускной способностью, допускающие подключение нового пользователя только после исключения старого); сети friend-to-friend (небольшие сети, чаще всего лично или дистанционно знакомых людей). С точки зрения легальности можно назвать: легальные сети (модерируемые, не подвергнутые блокировке), «серые» сети (со слабой модерацией, но удаляющие незаконный контент после жалоб пользователей), блокируемые сети (с блокировкой конкретным провайдером или в отношении которых Роскомнадзором принято решение о блокировке). При этом практика показывает, что на обход блокировки с помощью «зеркала», смены адреса, использования VPN-сервисов или специальных расширений браузеров требуется всего несколько дней.

Криминалистически значимыми задачами работы с распределенной информацией будут:

1) восстановление целого информационного объекта по частям;

2) установление самого пользователя и его идентификаторов;

3) доказывание осведомленности пользователя о содержании имеющихся у него информационных объектов;

4) доказывание умысла на распространение.

С криминалистической точки зрения особое значение приобретает специфика разделенного объекта. В отличие от классических вариантов восстановления целого по частям, как имеющим общую линию разделения, так и не имеющим таковой, или установления единого источника происхождения (емкости, объема или хранилища), распределенная информация, обнаруженная на разных устройствах, практически не имеет объединяющих признаков, объединение информационных объектов осуществляется программой-клиентом. При этом используются совершенно другие принципы и методы по сравнению с восстановлением целого по частям в ходе идентификационных или диагностических исследований материальных объектов.

Установление пользователя (конкретного терминала, с которого осуществлялась работа с информацией) осуществляется путем выявления идентификаторов — MAC-адреса (адреса компьютера или иного электронного устройства в киберпространстве), IP-адреса (совокупности кодов, указывающих «привязку» адреса в реальном пространстве), никнейма / логина / имени компьютера / имени пользователя (используются разные формулировки). В некоторых случаях при инсталляции программы-клиента требуется также указать язык пользователя. Что касается IP-адреса, то следует учитывать, что многими провайдерами по умолчанию предлагается пользователям динамический IP-адрес, а статический адрес предоставляется только за дополнительную плату. То есть динамический адрес может при каждом включении компьютера быть разным. Он присваивается службой DHCP в зависимости от политики присваивания адресов и наличия свободных адресов. Установив IP-адрес пользователя с помощью сервисов типа WhoIs, можно определить его географическую привязку. При этом с учетом практически полного отсутствия географических ограничений в киберпространстве расследование могут осложнять территориальная разнесенность пользователей на большие расстояния и нахождение пользователей в странах, не имеющих договоров о правовой помощи и о выдаче преступников с РФ, а также недружественно относящихся к России. Кроме того, пользователь может прибегнуть к использованию прокси-серверов. MAC-адрес компьютера тоже может быть изменен программными средствами.

Частично децентрализованные сети имеют единые хабы, на которых обрабатываются запросы пользователей на поиск определенной информации и, соответственно, оставляются виртуальные следы подобного поиска. В процессе взаимодействия с провайдерами и вла-

дельцами (модераторами) могут быть получены сведения о конкретных пользователях, интересующихся определенной информацией, списки запросов конкретного пользователя и т.д. Многие клиенты пиринговых сетей отображают не только никнеймы, но и IP-адреса владельцев информационных фрагментов. В некоторых программах национальная принадлежность пользователя дополнительно указывается флагом.

Нужно учитывать, что во многих случаях сам пользователь может достоверно не знать сущность информационного фрагмента, находящегося у него, или точное пофайловое содержимое крупного информационного пакета (крупного сборника документов, дискографии и т.д.). Следовательно, умысел на обладание определенной информацией, ограниченной в распространении, еще должен быть доказан. С учетом возможных стеганографических закладок это будет не всегда легкой задачей. Для ее решения важно будет восстановить историю поиска и перекачки.

Поскольку сам торрент непосредственно содержит только адреса владеющих нелегальной информацией пользователей, а не саму информацию, как верно отметил В. А. Мещеряков, «размер и вид этой информации не всегда позволяют ее однозначно связать с исходным файлом, являющимся объектом правовой охраны»[4]. Неполный информационный объект не может рассматриваться как целостный цифровой продукт.

Во многих клиентах скачанная информация автоматически ставится на раздачу. Поэтому распространение запрещенной информации (экстремистской, детской порнографии и т.д.) при подтверждении умысла на скачивание именно этого объекта не должно представлять больших сложностей.

Еще одну правовую и криминалистическую проблему подчеркнул В. А. Мещеряков — основанную на наличии информации о адресах владельцев частей информационного объекта в сети возможность перманентной перекачки и удаления после использования (просмотра, прочтения и т.д.) элементов информационного объекта, необходимых в конкретный момент. Он связывает эту возможность с наличием единого координирующего центра[5].

Ряд виртуальных следов может быть обнаружен на информационно-технологических устройствах подозреваемых — это следы установки и использования программ-клиентов файлообменных сетей и торрентов (ApexDC++, StrongDC++, µTorrent («мю-торрент»), uTorrent, BitTorrent), следы на рабочем столе, в папке установки, в реестре, списке автозагрузки, папках недавно использованных программ и файлов, следы в самих программах-клиентах, свидетельствующих о поиске и перекачке определенной информации. Кроме того, на терминале пользователя могут оставаться следы незаконченных перекачкой файлов пиринговой сети (например, *.!fl- в сети FlylinkDC++), файлов торрент-трекера, отражающих искомый информационный объект (это файлы с расширением *.torrent или .t_ с циферным кодом. В них содержится URL трекера, имя, размер файла и контрольные хеш-суммы SHA-1-сегментов раздаваемых файлов). В программах-клиентах пиринговой сети или торрентов может быть выявлена следующая информация: список скачиваемых, завершенных и раздающихся файлов, настройки раздачи (ограничения или полный запрет на раздачу), IP-адреса, с которых происходит скачивание, адреса трекеров, с которых производился поиск определенных файлов. Это дает возможность определить пользователей, стабильно раздающих незаконный контент. Кроме того, как отметил Д. А. Тарасов, «в торрент-файле содержатся следующие данные:

— announce — URL-адрес торрент-трекера;

— announce list — список, содержащий несколько URL-адресов трекеров;

— create date — дата создания торрент-файла;

— comment — комментарий от создателя торрент-файла;

— created by — название и версия программы, в которой был создан торрент-файл;

[4] *Мещеряков В. А.* Теоретические основы механизма следообразования в цифровой криминалистике : монография. М. : Проспект, 2022. С. 141.

[5] См.: *Мещеряков В. А.* Указ. соч. С. 142.

— info — директива для описания свойств файлов.

В файле истории торрент-клиента содержатся список загруженных с его помощью данных и путь их сохранения на компьютере пользователя (эти данные сохраняются, даже если загруженные файлы удалены и с носителя информации, и из списка загрузок в самом торрент-клиенте)»[6].

В России практически отсутствует правовая база для привлечения к ответственности провайдера пиринговых сетей (но и в сетях последнего поколения контроля за контентом сети у провайдера практически не остается). Отечественные авторы отрицают возможность привлечения к административной или уголовной ответственности администраторов файлообменной сети за размещение информации. Это связано с тем, что на сайтах торрентов размещается только информационный файл, который содержит информацию о «местонахождении ресурса сети Интернет (URL), информацию о закачиваемом файле (размер, длительность и т.д.), а также контрольную сумму файла (чтобы в итоге собрать все его части и получить единое целое). Отсюда можно сделать вывод, что администрация данного интернет-ресурса не может нести ответственность за нарушение авторских и смежных прав, так как ни в одном нормативном правовом акте не закреплен прямой запрет на размещение и распространение файлов, носящих информационный характер (файлы метаданных)»[7].

Между тем американский законодатель допускает ответственность провайдера за склонение (или содействие) к контрафакции, если провайдер был осведомлен о содержании файлов и оказал прямое материальное содействие. В Европе практикуется ответственности при осведомленности, материальной заинтересованности владельцев p2p-серверов и отсутствии своевременной реакции на законные требования об удалении контента.

Следует учитывать, что доступ к файлообменным сетям может быть различного уровня открытости, и если подключение к обычным пиринговым сетям или пиринговым сетям открытой авторизации оперативного сотрудника или следователя со своего устройства для изучения не будет создавать проблем, то для изучения сетей, требующих приглашения уже зарегистрированного пользователя, и сетей ограниченного круга пользователей friend-to-friend уже требуется серьезная агентурная работа по вербовке участника такой сети или внедрению оперативного сотрудника в связи с новинками разработок криптостойкости сетей.

С технической стороны для анализа пиринговых сетей применяются утилиты-сканеры, осуществляющие выборку и анализ данных о загруженных/розданных файлах, сканирующие логи программ-клиентов, в некоторых случаях осуществляющие поиск по логам нужных файлов (фильмов, музыки и т.д.).

Кроме того, для небольших файлообменных сетей остается достаточно актуальной схема доказывания, предложенная Н. Н. Федотовым. Он разграничивает доказывание факта размещения определенного информационного объекта в файлообменной сети и доказывание самого факта использования конкретным пользователем конкретной сети. В первом случае возможно использование заключения эксперта или свидетельских показаний. Для доказывания же второго обстоятельства Н. Н. Федотов предлагает разветвленную схему:

— «протокол экспертизы компьютера интересующего нас лица, содержащий вывод о том, что на исследуемом компьютере было установлено ПО файлообменных сетей и это ПО использовалось по назначению;

— показания иного участника файлообменной сети о том, что он взаимодействовал в этой сети с узлом, имеющим тот же IP-адрес, что использовался интересующим нас лицом;

---

[6] *Тарасов Д. А.* Об эффективности судебной компьютерной экспертизы в процессе доказывания деяний, связанных с «компьютерным пиратством» // Вестник Московского университета МВД России. 2017. № 2. С. 100.

[7] *Бакирова Е. Ю.*, *Свинарь А. Л.* Указ. соч. С. 27.

— протокол экспертизы компьютера иного участника файлообменной сети, содержащий вывод о том, что на исследуемом компьютере было установлено ПО файлообменных сетей, это ПО использовалось по назначению и обнаружены следы взаимодействия с IP-адресом интересующего нас лица;

— протокол осмотра или экспертизы компьютера оператора связи (провайдера), где зафиксировано наличие логов, отражающих информацию о трафике IP-адреса интересующего нас лица, причем в этом трафике присутствовали характерные для файлообменных сетей особенности (протоколы, порты, IP-адреса популярных узлов)»[8].

Зарубежные ученые подчеркивают необходимость изучения следующих файлов:

— файлов, которые являются либо контрабандными, либо незаконно хранящимися;

— конфигурационных файлов, содержащих информацию о сервере или пользователе, историю подключений, общие диски в сети или интернет-сайты, предоставляющие место для хранения данных вне сети (например, xDrive, Yahoo! и т.д.);

— файлов данных, показывающих расположение общего доступа к файлам с именами пользователей, паролями, условиями поиска, списками файлов, а также информацией о дате и времени (.dbb);

— файлов журналов, отображающих передачу данных и сетевую активность;

— сохраненной электронной почты, которая показывает соответствующую активность пользователя;

— программ передачи файлов[9].

В криминалистических целях можно выделить особые пиринговые сети, размещающие децентрализованные интернет-страницы на компьютерах громадного количества пользователей в сети в долях, так что установить конкретного владельца становится невозможно. В качестве примера таких сетей можно назвать тот же ZeroNet. А. Н. Колычева указывает, что «фактически его владельцем, как и “хостинг-провайдером”, становятся все пользователи децентрализованной сети, и только методом контент-анализа информации, в случае если на странице есть какие-то дополнительные сведения, например номера телефонов, почтовые адреса, адреса электронной почты, сетевые псевдонимы, определенная символика и т.д., можно выявить владельца»[10].

Подводя итог, можно отметить, что следователь в настоящее время уже должен быть не просто средненьким пользователем компьютера, но разбираться хотя бы на уровне терминологии и основ принципов функционирования всех этих новых информационных концептов. Представляется насущно необходимым организация периодических курсов повышения квалификации с рассмотрением новых технологий и основ их исследования. Ведь, как отмечает А. А. Куприянов, «для того чтобы привлечь квалифицированного специалиста, следователю приходится разбираться в том, кого именно привлечь в конкретном случае. Особенно актуальна эта проблема для уголовных дел о преступном распространении запрещенных материалов через файлообменные сети путем прямой рассылки или предоставления доступа»[11].

---

[8] *Федотов Н. Н.* Форензика — компьютерная криминалистика М. : Юридический мир, 2007. С. 244–245.

[9] *Hagy D. W*. Investigations Involving the Internet and Computer Networks. Washington, DC : National Institute of Justice, 2007. P. 52.

[10] *Колычева А. Н.* Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет : дис. … канд. юрид. наук. М., 2018. С. 56.

[11] *Куприянов А. А.* Доказывать отсутствие подделки IP-адресов обвиняемых обязано следствие // Уголовный процесс. 2017. № 6. С. 8.

БИБЛИОГРАФИЯ

1. *Бакирова Е. Ю.*, *Свинарь А. Л.* Защита авторских прав в сети Интернет на примере файлообменых сетей // Проблемы законодательного регулирования ресурсов и правового разрешения конфликтов с участием субъектов интернет-сообщества : материалы междунар. науч.-практ. конференции в рамках проекта «Российско-украинские криминалистические чтения на Слобожанщине», г. Белгород, 19 апреля 2013 г. / отв. ред. И. М. Комаров. — Белгород : НИУ «БелГУ», 2013. — С. 26–29.
2. *Войниканис Е. А.* Проблемы охраны результатов интеллектуальной деятельности в пиринговых сетях // Современное право. — 2009. — № 3. — С. 106–109.
3. *Колычева А. Н.* Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет : дис. … канд. юрид. наук. — М., 2018. — 199 с.
4. *Куприянов А. А.* Доказывать отсутствие подделки IP-адресов обвиняемых обязано следствие // Уголовный процесс. — 2017 — № 6.
5. *Мещеряков В. А.* Теоретические основы механизма следообразования в цифровой криминалистике : монография. — М. : Проспект, 2022. — 176 с.
6. *Радайкин М. Ф.* Правовое положение торрент-трекеров и их пользователей // Интеллектуальная собственность. Авторское право и смежные права. — 2013. — № 4. — С. 46–55.
7. *Тарасов Д. А.* Об эффективности судебной компьютерной экспертизы в процессе доказывания деяний, связанных с «компьютерным пиратством» // Вестник Московского университета МВД России. — 2017. — № 2. — С. 100–101.
8. *Федотов Н. Н.* Форензика — компьютерная криминалистика — М. : Юридический мир, 2007. — 432 с.
9. *Hagy D. W.* Investigations Involving the Internet and Computer Networks. — Washington, DC : National Institute of Justice, 2007. — 137 p.

Материал поступил в редакцию 6 марта 2024 г.

REFERENCES (TRANSLITERATION)

1. Bakirova E. Yu., Svinar A. L. Zashchita avtorskikh prav v seti Internet na primere fayloobmenykh setey // Problemy zakonodatelnogo regulirovaniya resursov i pravovogo razresheniya konfliktov s uchastiem subektov internet-soobshchestva: materialy Mezhdunar. nauch.-prakt. konferentsii v ramkakh proekta «Rossiysko-ukrainskie kriminalisticheskie chteniya na Slobozhanshchine», g. Belgorod, 19 aprelya 2013 g. / otv. red. I. M. Komarov. — Belgorod: NIU «BelGU», 2013. — S. 26–29.
2. Voynikanis E. A. Problemy okhrany rezultatov intellektualnoy deyatelnosti v piringovykh setyakh // Sovremennoe pravo. — 2009. — № 3. — S. 106–109.
3. Kolycheva A. N. Fiksatsiya dokazatelstvennoy informatsii, khranyashcheysya na resursakh seti Internet: dis. … kand. yurid. nauk (Ros. gos. un-t pravosudiya). — M., 2018. — 199 s.
4. Kupriyanov A. A. Dokazyvat otsutstvie poddelki IP-adresov obvinyaemykh obyazano sledstvie // Ugolovnyy protsess. — 2017 — № 6. — S. 8.
5. Meshcheryakov V. A. Teoreticheskie osnovy mekhanizma sledoobrazovaniya v tsifrovoy kriminalistike: monografiya. — M.: Prospekt, 2022. — 176 s.
6. Radaykin M. F. Pravovoe polozhenie torrent-trekerov i ikh polzovateley // Intellektualnaya sobstvennost. Avtorskoe pravo i smezhnye prava. — 2013. — № 4. — S. 46–55.
7. Tarasov D. A. Ob effektivnosti sudebnoy kompyuternoy ekspertizy v protsesse dokazyvaniya deyaniy, svyazannykh s «kompyuternym piratstvom» // Vestnik Moskovskogo universiteta MVD Rossii. — 2017. — № 2. — S. 100–101.
8. Fedotov N. N. Forenzika — kompyuternaya kriminalistika — M.: Yuridicheskiy mir, 2007. — 432 s.
9. Hagy D. W. Investigations Involving the Internet and Computer Networks. — Washington, DC: National Institute of Justice, 2007. — 137 p.