Баркалов Ю.М.,
Гайдин А.И.,
Потанина И.В.

ПРОЦЕССУАЛЬНЫЕ И ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ФИКСАЦИИ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ, ОБНАРУЖЕННОЙ В СЕТИ ИНТЕРНЕТ

Методические рекомендации

Издано в авторской редакции по решению методического совета института

Воронежский институт МВД России
2016

Авторы-составители:
Баркалов Юрий Михайлович
394065, Россия, Воронеж, пр. Патриотов, 53
Тел.: (473) 200-53-11
Гайдин Александр Иванович,
394065, Россия, Воронеж, пр. Патриотов, 53
Тел.: (473) 200-53-11
Потанина Ирина Витальевна,
394065, Россия, Воронеж, пр. Патриотов, 53
Тел.: (473) 200-52-43
E-mail: kriminalistika@vimvd.ru

Баркалов Ю.М., Гайдин А.И.,
Потанина И.В.

ПРОЦЕССУАЛЬНЫЕ И ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ФИКСАЦИИ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ, ОБНАРУЖЕННОЙ В СЕТИ ИНТЕРНЕТ

Методические рекомендации

Воронеж 2016

ББК 67.52

Рассмотрены и одобрены на заседании кафедры криминалистики. Протокол № 8 от 20.04.2016.

Рассмотрены и одобрены на заседании методического совета Воронежского института МВД России. Протокол № 9 от 23.05.16.

Рецензенты:

А.В. Пивовар – начальник следственной части по РОПД Главного следственного управления ГУ МВД России по Воронежской области, полковник юстиции;

О.К. Исаева – заместитель начальника отдела экспертно-криминалистических учетов ЭКЦ ГУ МВД России по Воронежской области, к.ю.н., подполковник полиции.

Баркалов, Юрий Михайлович. Процессуальные и организационно-тактические особенности фиксации доказательственной информации, обнаруженной в сети Интернет: методические рекомендации [электронный ресурс] / Ю.М. Баркалов, А.И. Гайдин, И.В. Потанина. – Электр. дан. и прогр. – Воронеж : Воронежский институт МВД России, 2016. – 1 электр. опт. диск (CD-ROM) : 12 см. – Систем. требования: процессор Intel с частотой не менее 1,3 ГГц ; ОЗУ 512 Мб ; операц. система семейства Windows ; CD-ROM дисковод.

ISBN 978-5-88591-381-2

В рекомендациях рассмотрены технические, процессуальные и тактические особенности фиксации доказательственной информации, хранящейся на ресурсах сети Интернет.

Рекомендации направлены на оптимизацию и повышение эффективности действий сотрудников полиции при производстве следственных действий в отношении криминалистически значимой информации, хранящейся на интернет-ресурсах.

ББК 67.52

ISBN 978-5-88591-381-2

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Возрастающая роль информационных технологий в деятельности современного общества и государства, стремительный рост числа преступлений, совершаемых с использованием компьютерной техники, оказывают существенное влияние на развитие системы средств и методов правоохранительной деятельности в сфере борьбы с преступностью. В нынешней ситуации особенно возрастает значение использования массивов криминальной и иной криминалистически значимой информации, хранящейся на различных ресурсах сети Интернет, для выявления, раскрытия и расследования преступлений.

Причинами востребованности у преступников Интернета является легкий доступ к широкой аудитории, обеспечение анонимной коммуникации, высокая скорость передачи информации и низкий уровень правового регулирования в этой сфере. Интернет является современным информационным пространством, которое стало альтернативой средств массовой информации и может эффективно использоваться правоохранительными органами. Одним из направлений реализации таких возможностей является обнаружение, фиксация и использование в доказывании криминалистически значимой информации, хранящейся на ресурсах сети. Развитие данного направления в деятельности полиции сталкивается с рядом проблем, ключевыми из которых являются низкий уровень научного, методического и технического обеспечения деятельности следственных, экспертных и оперативно-розыскных подразделений по использованию информационных ресурсов в выявлении, раскрытии и расследовании преступлений и пробелы правового регулирования общественных отношений в сфере доказывания по уголовным делам. На это в своих работах неоднократно указывали ученые-криминалисты В.А. Мещеряков, С.В. Зуев, А.М. Багмет и др.[1]

[1] См.: Зуев С.В., Сутягин К.И. Электронное копирование информации как самостоятельное следственное действие // Следователь. –2003. – № 4; Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе: монография. – М.: Юрлитинформ, 2012. – 152 с.; Багмет А.М., Скобелин С.Ю. Извлечение данных из электронных устройств как самостоятельное следственное действие // Право и кибербезопасность. – 2013. – № 2. – С. 22-27; Мещеряков В.А. Понятие и виды

Проведенное нами исследование в рамках обозначенной темы направлено на решение одной из указанных проблем – методического обеспечения деятельности следственных подразделений органов внутренних дел при производстве следственных действий, связанных с фиксацией информации, хранящейся на ресурсах сети Интернет, с целью её использования в качестве доказательств с учетом современного уголовно-процессуального регулирования данных правоотношений.

В исследовании решались задачи определения ресурсов сети Интернет, имеющих наибольшее значение в качестве источника доказательственной информации по уголовным делам, и их особенностей, оказывающих влияние на тактику и способы фиксации; выявления основных направлений использования информации, полученной из сетевых источников, в расследовании отдельных видов преступлений с учетом её характера и способов фиксации; установления возможностей и роли специалиста, привлекаемого к действиям, связанным с обнаружением и фиксацией криминалистически значимой информации на ресурсах Интернета; формирования рекомендаций тактического и технического характера по фиксации информации в электронном виде с сетевых ресурсов путем протоколирования, изъятия электронного носителя и копирования данных.

следственного осмотра при расследовании преступлений в сфере использования информационно-коммуникационных технологий // Библиотека криминалиста. – 2014. – №5.

1. ПРАВОВЫЕ И КРИМИНАЛИСТИЧЕСКИЕ ОСНОВЫ ФИКСАЦИИ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ, ХРАНЯЩЕЙСЯ НА РЕСУРСАХ ИНТЕРНЕТА

Многообразие источников криминалистически значимой информации в Интернете, правовые и технические особенности функционирования данной среды, механизм образования «виртуальных следов» — это факторы, которые предопределяют насущную потребность разработки средств, методов и приемов собирания и исследования доказательств в электронном виде, хранящихся на ресурсах сети. В процессе решения данной задачи авторы столкнулись с рядом проблем, преодоление которых способствовало формированию тактических рекомендаций по фиксации доказательственной информации с ресурсов Интернета.

Первая проблема заключается в уяснении структуры и особенностей ресурсов Интернета, на которых может быть обнаружена информация, имеющая доказательственное значение. Вид ресурса определяют технические и программные особенности обращения информации, ее характер и правовые аспекты организации и функционирования ресурса, а также защиты информации. Перечисленные характеристики оказывают влияние на выбор тактики действий по собиранию доказательств. В данной работе мы не преследуем цель дать исчерпывающее описание информационных ресурсов сети Интернет. Наша задача – указать отличительные особенности тех из них, использование которых в доказывании по уголовным делам более эффективно.

Наиболее востребованными у пользователей и содержащими наибольший объем значимой в раскрытии и расследовании информации являются электронная почта и веб-ресурсы.

Электронная почта – это ресурс, обеспечивающий передачу почтовых сообщений (писем) электронным способом. С ее помощью можно передать сообщение в любой конец света не более чем за сутки. Это время зависит от используемого способа передачи. Для отправки сообщений по электронной

почте необходимо только одно – адрес получателя (E-mail адрес). Сообщения электронной почты могут содержать небольшие по объему тексты или полностью сформированные объемные документы и включать вложения файлов различных форматов. Порядок получения сообщения по электронной почте напоминает корреспонденцию «до востребования»: полученное на адрес E-mail письмо хранится на сервере провайдера.

При установлении связи и предъявлении полномочий (логина и пароля) все сообщения могут быть переданы на компьютер пользователя, также возможно ознакомление с их содержанием непосредственно на сервере.

Веб-ресурсы или всемирная паутина (WWW) – это единое информационное пространство, состоящее из сотен миллионов взаимосвязанных электронных документов, хранящихся на веб-серверах. Отдельные документы, составляющие пространство веб, называют веб-страницами. Группы тематически объединенных веб-страниц называют веб-узлами (жаргонный термин — веб-сайт или просто сайт). Веб-страница – это своего рода документ, хранящийся на компьютере, подключенном к Интернету. Этот документ имеет специальный формат (формат HTML), каждая страница имеет свой уникальный адрес URL. Подключенный к сети Интернет компьютер, на котором хранятся веб-страницы, называется физическим веб-сервером или веб-узлом. Из всего многообразия различных сайтов и порталов необходимо выделить социальные интернет-сети, видеохостинги, интернет-магазины и веб-форумы. Именно на данных сайтах прежде всего можно обнаружить информацию, имеющую доказательственное значение.

Социальные сети представляют собой автоматизированные веб-сервисы, предполагающие авторизацию (создание и использование учетной записи (аккаунта)) и коммуникацию в рамках тематических (гендерных, возрастных, образовательных и иных) интернет-сообществ (система «друзей» и «групп»). Внутри данных ресурсов реализованы технологические решения, обеспечивающие мгновенный обмен сообщениями, фолксономию (народную классификацию, например, с использованием тегов, т.е. меток, ключевых слов),

синдикацию (одновременное распространение информации на различных веб-страницах), мэшап (использование информации с других веб-источников), AJAX (асинхронную загрузку данных на страницу без её перезагрузки) и другие.

Видеохостинг – сайт, позволяющий загружать и просматривать видео в браузере, например, через специальный проигрыватель. При этом большинство подобных ресурсов не предоставляют видео, следуя таким образом принципу User-generated content (различный медиа-контент, который создается конечными пользователями).

Интернет-магазин (англ. online shop или e-shop) — сайт, торгующий товарами посредством сети Интернет. Позволяет пользователям онлайн, в своём браузере или через мобильное приложение сформировать заказ на покупку, выбрать способ оплаты и доставки заказа, оплатить заказ.

Веб-форум — разновидность веб-ресурса для организации общения посетителей веб-сайта. Суть работы форума заключается в создании пользователями (посетителями форума) своих тем с их последующим обсуждением путём постинга размещения сообщений внутри этих тем. Отдельно взятая тема, по сути, представляет собой тематическую гостевую книгу.

Еще одним ресурсом Интернета являются ftp-серверы. FTP – протокол передачи файлов, который позволяет пользователю копировать файлы из одного подключенного к сети Интернет компьютера в другой. Программное обеспечение FTP разделено на две части: одна выполняется на компьютере, который содержит файлы (ftp-сервер), а другая – на компьютере, которому эти файлы требуются (клиент). Данный сервер содержит информацию в виде файловой структуры. На ftp-сервер провайдер или пользователи выкладывают разнообразные файлы (антивирусы, полезные программы, иногда – фильмы и музыку), чтобы ими могли воспользоваться посетители сервера. Несмотря на то, что адресация такого рода серверов осуществляется посредством URL, представление информации в виде файловой структуры не позволяет отнести данный ресурс к числу веб-сайтов.

Иным ресурсом хранения и обмена файлами являются пиринговые сети (P2P). По своей сути они представляют собой объединение компьютеров, которое базируется исключительно на равноправии всех участников, называемых в таких системах пирами. От клиент-серверной архитектуры, лежащей в основе построения ресурса обмена файлами через FTP-протокол, такие сети отличаются непосредственно тем, что подобная организация способна сохранить работоспособность совершенно всей пиринговой сети при любом количестве доступных узлов (пиров), а также при любом их сочетании.

Еще более современным и набирающим популярность сервисом, который дает возможность хранить, обмениваться информацией и обрабатывать ее, является облачное хранилище данных. Это модель онлайн-хранилища, в котором данные хранятся на многочисленных распределённых в сети серверах, предоставляемых в пользование клиентам в основном третьей стороной. В отличие от модели хранения данных на собственных выделенных серверах, приобретаемых или арендуемых специально для подобных целей, количество или какая-либо внутренняя структура серверов клиенту в большинстве случае не видна. Данные хранятся и обрабатываются в так называемом «облаке», которое представляет собой с точки зрения клиента один большой виртуальный сервер. Физически же такие серверы могут располагаться удалённо друг от друга географически, вплоть до расположения на разных континентах.

Разговор через Интернет или Chat – это ресурс, обеспечивающий способ общения посредством набираемого на клавиатуре текста, который пользователь отправляет в некоторую область сети, называемую каналом (Channel). Этот текст становится доступным для чтения всем, кто в данный момент присоединяется к этому каналу. Иначе говоря, Chat дает возможность прямого разговора через текст на мониторе.

Дальнейшее развитие метода состоит в возможности прямого разговора по принципу телефона – IP-телефония. Это телефонная связь по протоколу IP. Под IP-телефонией подразумевается набор коммуникационных протоколов, технологий и

методов, обеспечивающих традиционные для телефонии набор номера, дозвон и двустороннее голосовое общение, а также видеообщение по сети Интернет.

Целесообразность использования в раскрытии и расследовании преступлений сведений, размещенных на ресурсах сети Интернет, обуславливается тем, что такого рода информация может существенно облегчить выбор направлений поисковой деятельности, а также планирование проведения оперативно-розыскных и следственных мероприятий; поиск информации на открытых ресурсах быстрее, а иногда и эффективнее, чем при добывании ее с помощью негласных мероприятий; в условиях дефицита времени такие источники являются единственным средством быстрого получения необходимой информации; зафиксированные сведения, содержащиеся на ресурсах Интернета, можно использовать для выявления иной криминалистически значимой информации, относящейся к расследуемому событию.

Следующим важным аспектом, определяющим способ и тактику фиксации доказательственной информации, хранящейся на ресурсах Интернета, является направление её использования при расследовании различных видов преступлений. В частности, представление о том, какие обстоятельства расследуемого преступления могут быть установлены при использовании той или иной информации из сети, какие конкретные задачи (тактические или методические) могут быть решены при использовании различных сведений, определяет выбор следователем времени, формы, способа и средств фиксации доказательственной информации.

Сетевая социальная среда крайне разнородна, и определенная ее часть, разделяющая социально опасные взгляды, может рассматриваться в качестве криминогенной среды. Принадлежащие к ней субъекты объединяются в маргинальные группы. Комфортные условия, которые предоставлены в сетевом пространстве таким негативно настроенным сообществам, приводят к появлению в нем многочисленных зон общения личностей с отклоняющимся поведением. При этом, например, происходит увеличение количества сетевых ресурсов, носящих экстремистскую направленность. Растет число сайтов,

принадлежащих организованным преступным формированиям, через которые они не только обмениваются информацией, но и пытаются популяризировать свои идеи и образ жизни. В сетевом пространстве формируется международный рынок детской порнографии как один из самых прибыльных секторов теневой экономики. Возможности Интернета широко используются для распространения информации о местах сбыта наркотических средств, рекомендаций по их изготовлению. Через глобальную сеть осуществляется торговля оружием, похищенными номерами кредитных карт. Участились случаи размещения в Интернете видеосъемок реальных сцен насилия (например, садистских избиений случайных прохожих, снятых на камеры мобильных телефонов)[2]. Распространение систем видеорегистрации в помещениях, на улице и транспорте повлекло рост количества видеороликов, выложенных пользователями на ресурсах сети, в которых запечатлены факты имущественных преступлений, преступлений против личности, общественного порядка и связанные с нарушением правил дорожного движения. Все эти записи имеют потенциальное доказательственное значение и могут быть использованы в расследовании.

Сетевые информационные ресурсы становятся источником общественно опасных знаний: здесь приводятся описания способов суицида, получения взрывчатых и отравляющих веществ, пропагандируются разврат, каннибализм и т.п.

Из всего многообразия преступлений, при расследовании которых применяются доказательства, полученные с ресурсов Интернета, в зависимости от их доли в числе иных доказательств необходимо выделять так называемые сетевые преступления, возможность совершения которых обусловлена существованием самой глобальной сети, преступления, совершаемые с использованием возможностей сети Интернет, и преступления, доказательства по которым можно обнаружить на ресурсах сети.

[2] Ишин А.М. Современные проблемы использования сети интернет в расследовании преступлений // Вестник Балтийского федерального университета им. И. Канта. – 2013. – № 9. – С. 34.

При расследовании сетевого мошенничества следы преступной деятельности могут быть обнаружены на достаточно большом числе ресурсов Интернета. Планируя деятельность по обнаружению и фиксации доказательственной информации, необходимо учитывать, что действия по осуществлению мошеннической комбинации в сети Интернет условно можно разделить на две стадии:

– передача или навязывание ложной информации потерпевшим с целью введения их в заблуждение;

– непосредственное завладение предметом посягательства.

Наиболее распространенными способами передачи ложной информации являются мошеннические сайты и электронная почта. Однако мошенники могут использовать интернет-пейджеры (ICQ), форумы или чаты.

Веб-сайт, как правило, регистрируется на бесплатном хостинге, чтобы соблюсти анонимность. Однако мошенники могут разместить сайт и на серверах хостинг-компаний, представляющих платные услуги.

Непосредственное завладение предметом посягательства может осуществляться путем ввода регистрационных данных кредитных карт, переводом средств на «электронные кошельки», номера сотовых телефонов и т.п. Перевод электронных денег (WebMoney, Яндекс-деньги) наиболее характерен для схем с предоплатой (сотовое мошенничество, предложение несуществующих товаров). В отличие от традиционного мошенничества, характерной особенностью интернет-мошенничества является то обстоятельство, что при нем остается мало традиционных следов и потерпевшие не знают преступников в лицо.

При совершении мошенничества и других сетевых преступлений организованными группами, имеющими международный состав, выход за пределы национальных границ и использование ими возможностей глобальной информационной сети Интернет обусловлены прежде всего взаимосвязанным процессом экономической и криминальной глобализации.

Международные компьютерные сети позволяют осуществлять деятельность на такой территории, где может действовать (намеренно или непреднамеренно) принцип экстерриториальности. Правоохранительные органы могут в данном случае осуществлять обмен информацией, хотя расцениваться с правовой точки зрения эта информация может по-разному, в зависимости от особенностей национального законодательства.

Общепризнано, что государство правомочно производить на своей территории следственные действия или применять принудительные меры в отношении любого из своих граждан. В результате применения таких полномочий могут возникать случаи, когда размещенные на другой территории данные считываются и копируются или, возможно, уничтожаются. С точки зрения государства, в котором велся поиск данных, такие действия могут образовывать состав уголовного преступления в соответствии с внутренним уголовным правом, а также являться нарушением национального суверенитета.

В то же время международное право не запрещает подобное вмешательство, поскольку с технической точки зрения такие данные доступны и могут быть получены из государства, осуществляющего их поиск, без какой-либо помощи или вмешательства со стороны государства, где осуществляется поиск таких данных. Имеющиеся в любых разделах сети данные можно рассматривать как общедоступные, и по этой причине вопрос о доступе к ним из любого государства, в котором они в настоящее время находятся, регулируется исключительно внутренним, а не международным правом. С такой точки зрения обращение к государству, где осуществляется поиск данных, не является необходимым ни на одном из этапов деятельности.

При расследовании имущественных преступлений с использованием сети Интернет, носящих трансграничный характер, сведения, хранящиеся на её ресурсах, могут быть использованы и для установления потерпевших, что очень часто вызывает массу трудностей. Сообщения о совершении в отношении конкретных физических и юридических лиц преступлений можно обнаружить на форумах, в гостевых книгах на сайтах, в чатах, на страницах социальных сетей.

Важнейшим доказательством преступного распространения порнографических материалов через сеть Интернет являются сами файлы видеозаписей, фотоснимков, зафиксированные на сайтах, ftp-серверах в пиринговых сетях, облачных хранилищах. Также доказыванию способствует фиксация на веб-ресурсах рекламы порнографических материалов.

Расследование незаконного оборота наркотических средств и психотропных веществ, совершаемого с использованием современных способов коммуникации между распространителями и потребителями, сталкивается с новыми способами сокрытия следов преступной деятельности путем передачи сообщений (в том числе кодированных) в электронной переписке. Таким образом передается информация о банковских счетах, координатах тайников или мест закладок, способах изготовления наркотиков и так далее. При создании сайтов, через которые реализуются наркотики, наиболее часто применяются следующие способы электронной конспирации: предоставление заведомо неверных регистрационных данных; использование данных подставных лиц; использование похищенных реквизитов доступа в сеть Интернет; переадресация обращений пользователей; периодическая смена места размещения ресурса. Указанные способы существенным образом затрудняют расследование уголовных дел данной категории. К задачам фиксации следов противоправной деятельности, имеющихся на такого рода сайтах, добавляется необходимость установления конкретных лиц, создавших и использовавших соответствующий ресурс.

Информация, содержащаяся в аккаунтах социальных интернет-сетей, является важным объективным источником информации о личности как подозреваемых, так и иных участников судопроизводства. Фиксация факта общения в сети, наличия лиц в «друзьях», общие фотографии могут быть использованы для доказывания мотива преступления, наличия личной заинтересованности в ходе расследования и других обстоятельств, а могут быть положены в основу принятия решения о производстве следственных действий

(обыска, допроса, контроля и записи телефонных и иных переговоров и др.) и оперативно-розыскных мероприятий.

Важным условием в выборе способа и тактики фиксации доказательственной информации является обеспечение своевременного закрепления доказательств в электронном виде, отличающихся значительной динамичностью, особенно в условиях противодействия со стороны заинтересованных лиц. Оценка результата возможного противодействия расследованию преступлений имеет большое значение для планирования и организации работы следователя. При оказании такого противодействия в сфере компьютерной информации каждый очередной удачный факт сокрытия преступления позволяет правонарушителю осознать, насколько примененные им методы были адекватны поставленной задаче, и на основании этого решить вопрос о возможности применения новых. Кроме того, каждый случай подобного рода действий – это возможность для преступника еще лучше освоиться в виртуальной среде компьютерной информации. При этом он оценивает то, какие средства являются наиболее эффективными для достижения поставленных им преступных целей, при необходимости эти средства тиражирует и совершенствует.

Значительную роль может играть информация, хранящаяся на ресурсах сети Интернет, при организации и осуществлении розыска. По отношению к объектам розыска информация в электронном виде бывает: непосредственно с ними связанная и вспомогательная или ориентирующая – указывающая на разыскиваемый объект и (или) иные объекты, связанные с событием преступления.

Использование конкретных способов и средств фиксации информации, хранящейся на ресурсах сети Интернет, должно обеспечивать получение сведений, обладающих свойствами доказательств.

Проблемы с признанием данных в электронном виде в качестве доказательств связаны с наличием стойких предубеждений в среде юристов, что электронно-цифровая форма фиксации информации позволяет вносить невыявляемые изменения, а это несопоставимо с таким свойством доказательств,

как достоверность, и что невозможность идентификации записывающего оборудования несопоставима с таким свойством доказательств, как относимость.

Решение данной проблемы возможно при комплексном подходе, где сочетаются технические методы, делающие невозможным сам факт внесения изменений, и тактические, использующие процессуальные возможности обеспечения достоверности и допустимости доказательств.

К тактическим приемам можно отнести использование определенных форм процессуального обеспечения подлинности результатов, например производство действий при понятых, упаковка носителей информации, исключающая её вскрытие без нарушения целостности и обеспечивающая невозможность иного внепроцессуального воздействия на саму информацию, записанную на носитель, и др.

Следователь при производстве отдельных следственных действий может применять несколько различных способов фиксации доказательственной информации в электронном виде. Обязательным способом выступает протоколирование следственного действия. Вспомогательными способами выступают изъятие электронного носителя информации и копирование криминалистически значимой информации на иной носитель. Средства фото- и видеосъемки используются для фиксации хода следственного действия, а при условии демонстрации данных на мониторе компьютера – и для их фиксации.

Электронный носитель, который используется для копирования, сам по себе не имеет никакого отношения к событию преступления, не связан с ним, выбор его зависит от материально-технической базы следствия и эффективности применения ее в конкретной ситуации.

Зафиксированные таким образом сведения относятся к категории вещественных доказательств, так как они обладают признаками, присущими исключительно вещественным доказательствам:

– данные, имеющие отношение к делу, содержатся на них во внешних признаках (в зависимости от способа записи бинарного кода);

– могут служить средством к обнаружению преступления, установлению фактических обстоятельств дела, выявлению виновных либо к опровержению обвинения или смягчению ответственности;

– в них реализован материальный способ получения, сохранения и передачи невербальной информации, имеющей отношение к делу.

При копировании данных с целью фиксации доказательственной информации в электронном виде возникают так называемые производные вещественные доказательства. Несмотря на то, что новый носитель информации отличается от первоначального тем, что может быть изготовлен из других материалов, иметь другой вес, цвет, форму, размер и т.п., использование специальных средств и методов, применяющихся при копировании, позволяет достаточно точно передать характер тех признаков в зафиксированных данных, которые имеют доказательственное значение. Кроме уже указанных выше причин использования электронных носителей информации в качестве производных вещественных доказательств, может возникнуть необходимость использовать их в качестве первоначальных, если в процессе производства будет установлены умышленные действия, направленные на уничтожение носителя или самих данных, а также в случае их модификации.

Достаточную сложность использования в доказывании представляют производные доказательства в электронном виде, полученные в результате фиксации данных, хранящихся на интернет-ресурсах с использованием DLP-систем. Эти системы используются для предотвращения утечки данных и являются действенным средством фиксации криминалистически значимой информации, особенно при расследовании преступлений в сфере компьютерной информации, экономических, налоговых и должностных преступлений. Они активно внедряются в целях выявления и блокирования нелегитимной передачи информации из защищенных автоматизированных систем. Основными функциями DLP-системы являются: централизованное управление, настройка политик безопасности, блокирование

несанкционированных перемещений данных, создание цифровых отпечатков документов[3], формирование отчетов о работе системы.

DLP-система представляет собой комплекс программно-аппаратных средств, обеспечивающих защищенность информации от угроз нелегитимной передачи из защищенного сегмента автоматизированной системы путем анализа и блокирования исходящего трафика. Условно DLP-системы разделяют на три типа: системные (уровня хоста), сетевые, прикладные (как правило, уровня СУБД). Независимо от типов DLP-систем, используемые методы анализа данных разделяют на атрибутные (например, использующие свойства объектов системы) и семантические (основанные на смысловом анализе информации, как правило, путем выявления сочетаний ключевых данных). В настоящее время большинство корпоративных DLP-систем являются комплексными и включают следующие компоненты: модуль централизованного управления, агенты рабочих станций (серверов), модули анализа протоколов, модули сканирования (поиска) данных[4].

Так, Банк России рекомендовал российским банкам следить за своими сотрудниками, чтобы предотвратить утечки пользовательских данных. С 1 июня 2014 года банкиры обязаны анализировать переписку своих подчиненных и их перемещение по интернет-сайтам, что, соответственно, и подразумевает использование в банках систем DLP. Стандарт обеспечения информационной безопасности, подготовленный Центробанком, требует, например, архивировать электронную почту, чтобы после утечки можно было провести внутреннее расследование, а также использовать защищенные сетевые протоколы при выходе

[3] Матвеев В.А., Медведев Н.В., Троицкий И.И., Цирлов В.Л. Состояние и перспективы развития индустрии информационной безопасности Российской Федерации в 2011 г. // Вестник МГТУ им. Н.Э. Баумана. Сер. «Приборостроение». Спецвыпуск «Технические средства и системы защиты информации». – М., – 2011. – С. 3–6.

[4] Барабанов А.В., Гришин М.И., Марков А.С., Цирлов В.Л. Формирование требований по безопасности информации к DLP-системам // Вопросы радиоэлектроники. – 2013. – №2. – С. 67-76.

информации за пределы контролируемой зоны[5]. Указанная информация может способствовать раскрытию и расследованию преступлений.

Но вопрос допустимости использования DLP-решений в уголовном процессе остаётся достаточно острым, так как сама проблема контроля за перепиской работников неоднозначна.

С одной стороны, собственником компьютеров, сервера электронного ящика, точек доступа в Интернет является работодатель. Из этого следует и право компании контролировать процесс использования работниками принадлежащего ей имущества в соответствии с его целевым назначением (ч. 2 ст. 209 ГК РФ). Кроме того, одной из трудовых обязанностей работодателя является обязанность обеспечить работника оборудованием, инструментами, технической документацией и иными средствами, необходимыми ему для исполнения трудовых обязанностей (ст. 22 ТК РФ). Этой обязанности работодателя корреспондирует обязанность работника добросовестно исполнять свои трудовые обязанности, возложенные на него трудовым договором, соблюдая при этом правила внутреннего трудового распорядка (ст. 21, ч. 1 ст. 189 ТК РФ).

Но, с другой стороны, статьей 23 Конституции РФ гарантировано право каждого на неприкосновенность частной жизни, тайны переписки, телеграфных и иных сообщений. Этот же принцип защиты тайны связи реализован в нормах статьи 63 Федерального закона от 07.07.03 № 126-ФЗ «О связи» и статьи 138 Уголовного кодекса, устанавливающей уголовную ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Ограничение тайны переписки допускается только в случаях, предусмотренных федеральными законами.

Соответственно, при решении вопроса о возможности использования информации, полученной при осуществлении контроля работодателем за корпоративной перепиской сотрудников, нужно понять, где проходит граница между частной жизнью работника и его рабочими обязанностями,

[5] Юзбекова И., Алешкина Т. Центробанк рекомендовал российским банкам следить за своими сотрудниками // РБК daily URL: http://rbcdaily.ru/media/ 562949991666877 (дата обращения:06.06.2015)

если речь идет о сообщениях, которыми он обменивается с корпоративной почты (своего рабочего места).

Так, в соответствии с решением Европейского суда по правам человека по делу «Копланд против Соединенного Королевства»[6], работодатель не может контролировать электронную переписку работников, если не соблюден ряд условий. Электронные сообщения, отправленные с работы, должны быть защищены аналогичным образом, как и информация, полученная в результате мониторинга личного использования Интернета. Таким образом, ЕСПЧ распространил конституционные принципы соблюдения тайны переписки и неприкосновенности частной жизни при пользовании Интернетом и электронной перепиской вне рамок трудовых отношений на аналогичные действия, совершаемые в те часы, когда работник выполняет или должен выполнять трудовые обязанности. При этом ЕСПЧ обосновал свое решение о том, что вмешательство в личную жизнь Копланд не соответствовало закону, тем, что отсутствовали данные о существовании в период событий каких-либо положений в общем законодательстве страны или локальных нормативных актах по месту работы, устанавливавших обстоятельства, которые давали работодателю право осуществлять мониторинг использования работниками телефона, электронной почты и Интернета.

Таким образом, из приведенного выше решения ЕСПЧ № 62617/00 следует, что право работодателя контролировать переписку работника не исключается полностью. Однако это право должно быть закреплено в нормативном правовом акте или хотя бы в локальном нормативном акте. В частности, право работодателя на контроль за электронными сообщениями работников, которые отправляются с корпоративных адресов электронной почты, может быть установлено в Правилах внутреннего трудового распорядка

[6] Копланд против Соединенного Королевства (Copland v. United Kingdom) Постановление Европейского Суда по правам человека от 3 апреля 2007 года (жалоба № 62617/00). // Бюллетень Европейского Суда по правам человека", – 2007, – № 10.

организации наряду с обязанностью работника использовать электронную почту только в рабочих целях (ч. 4 ст. 189 ТК РФ)[7].

Анализ приведенного решения ЕСПЧ позволяет сделать вывод о необходимости соблюдения и еще одного условия легитимности получения таких сведений – это получение согласия работника на осуществление контроля за его электронной перепиской или по крайней мере осведомленности работника об этом факте.

Согласно разъяснениям, приведенным Пленумом Верховного Суда РФ, доказательства должны признаваться полученными с нарушением закона, если при их собирании и закреплении были нарушены гарантированные Конституцией РФ права человека и гражданина или установленный уголовно-процессуальным законодательством порядок их собирания и закрепления, а также если собирание и закрепление доказательств осуществлено ненадлежащим лицом или органом либо в результате действий, не предусмотренных процессуальными нормами.

Таким образом, можно сделать вывод, что информация, полученная в результате использования работодателем DLP-систем, может быть использована в качестве доказательств по уголовному делу только в случае легитимного применения работодателем этих систем. Это в свою очередь предусматривает наличие локального нормативного акта, регламентирующего использование DLP-систем данным учреждением, а также осведомлённости работника о контроле его активности в сети Интернет с использованием этих систем и получение от него согласия на осуществление такого контроля.

Еще одним важным условием эффективной фиксации для целей доказывания информации хранящейся на ресурсах сети Интернет, является наличие у следователя необходимого объема знаний и навыков работы с электронными доказательствами. С этим связано наличие знаний о возможностях работы в Интернете, порядке доступа к сети, отыскания,

[7] Каспаров С. Проверка электронной почты сотрудников. Как контролировать переписку на законных основаниях. // Электронный ресурс: Петербуржский правовой портал. URL: http://ppt.ru/news/117831 (дата обращения: 06.06.2015).

получения и оценки информации. Помимо технических тонкостей работы в поисковых порталах, следователь должен владеть навыками умелого вычленения ключевых слов, знать орфографию, обладать способностью определить нужный источник по минимуму информации о нем, выведенной на страницу поискового портала. В отдельных случаях было бы полезным и знание иностранных языков или хотя бы наличие навыков работы с программами-переводчиками.

Таким образом, на сегодняшний день содержащими наибольший объем значимой в раскрытии и расследовании информации, которая может использоваться в качестве доказательственной, являются следующие интернет-ресурсы: электронная почта, социальные интернет-сети, видеохостинги, интернет-магазины, веб-форумы, ftp-серверы, пиринговые сети, облачные хранилища информации и чаты.

Целесообразность использования в раскрытии и расследовании преступлений сведений, размещенных на ресурсах сети Интернет, обуславливается тем, что такого рода информация может существенно облегчить выбор направлений поисковой деятельности, а также планирование проведения оперативно-розыскных и следственных мероприятий; поиск информации на открытых ресурсах быстрее, а иногда и эффективнее, чем при добывании ее с помощью негласных мероприятий; в условиях дефицита времени такие источники являются единственным средством быстрого получения необходимой информации; зафиксированные сведения, содержащиеся на ресурсах Интернета, можно использовать для выявления иной криминалистически значимой информации, относящейся к расследуемому событию.

Из всего многообразия преступлений, при расследовании которых применяются доказательства, полученные с ресурсов Интернета, в зависимости от их доли в числе иных доказательств необходимо выделять так называемые сетевые преступления, возможность совершения которых обусловлена существованием самой глобальной сети, преступления, совершаемые с

использованием возможностей сети Интернет, и преступления, доказательства по которым можно обнаружить на ресурсах сети.

Факторами, определяющими способ и тактику фиксации доказательственной информации из сети, являются технические и программные особенности обращения информации на конкретных ресурсах и ее характер, правовые аспекты организации и функционирования ресурса, а также защиты информации, направления ее дальнейшего использования в расследовании преступлений, обеспечение своевременности фиксации данных.

Обеспечение достоверности и допустимости доказательств из сети Интернет при производстве следственных действий осуществляется в рамках комплексных подходов, сочетающих технические методы, делающие невозможным сам факт внесения изменений в фиксируемые данные, и тактические приемы производства следственных действий. Определённую сложность в доказывании представляет использование информации в электронном виде, полученной в результате фиксации данных, хранящихся на интернет-ресурсах, с использованием DLP-систем, использующихся в целях выявления и блокирования нелегитимной передачи сведений из защищенных автоматизированных систем.

2. ТЕХНИЧЕСКИЕ И ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ФИКСАЦИИ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ С СЕТЕВЫХ РЕСУРСОВ ИНТЕРНЕТА ПРИ ПРОИЗВОДСТВЕ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ

Фиксации доказательств в сети Интернет предшествует поиск криминалистически значимой информации на сетевых ресурсах. Субъектами поиска могут выступать сотрудники оперативных подразделений органов внутренних дел, следователи и дознаватели. Возможности оперативных сотрудников шире за счет использования негласных оперативно-розыскных мероприятий и специализированного программного обеспечения. Однако реализация криминалистических рекомендаций по осуществлению поисковой и розыскной деятельности в сети тоже позволяет следователям и дознавателям вполне успешно решать задачи обнаружения необходимой информации.

Поиск по информационным ресурсам Интернета может быть реализован через различного рода поисковые системы (Google, Yandex, Rambler и т.п.), использующие производительные алгоритмы обнаружения информации по заданным реквизитам. В ходе информационного поиска выявляются сайты, связанные с преступной деятельностью, а также сетевые ресурсы, содержащие запрещенную к распространению информацию.

Поисковые серверы могут применяться также для получения дополнительной информации о пользователе или группе пользователей сети. Сведения об участниках судопроизводства возможно получить в открытом доступе на их личных страницах в социальных сетях (Одноклассники.ру, ВКонтакте.ру) либо в персональных блогах.

Повышение эффективности интернет-мониторинга предполагает применение контент-анализа, который представляет собой формализованный аналитический метод исследования содержания документов в целях выявления и измерения характеристик социальных явлений, получивших в них отражение. Основными объектами такого анализа могут быть сетевые информационные

ресурсы и тексты в местах сетевого общения (социальные сети, блоги, форумы и т.п.) криминальной направленности.

Контент-анализ позволяет установить присутствие в тексте или массивах текстов ключевых слов, зафиксировать смысловые единицы содержания, частоту их употребления, соотношение различных элементов текста.

Наиболее широкие возможности контент-анализа социальных сетей представляет использование программного обеспечения UFED, Мобильный криминалист, XRY, U2. Сопоставление и обобщение полученных материалов позволяет установить связи лиц, их контакты, выявить криминальные социальные группы и т.д.

Для поиска информации оптимально использовать языковые запросы, что позволит исключить сайты и данные, не относящиеся к преступной деятельности. Такой поиск не требует материальных затрат на приобретение специализированного программного и программно-аппаратного обеспечения. Выявленная информация должна анализироваться на предмет ее достоверности (корректность), объективности и однозначности.

Ниже приведены синтаксисы языковых запросов Yandex и Google. (таблицы 1, 2)

Синтаксис языковых запросов Yandex

Синтаксис	**Значение оператора**
пробел, &	Логическое И (в пределах предложения)
|	Логическое ИЛИ
+	Обязательное наличие слова в найденном документе
~	Бинарный оператор И НЕ (в пределах предложения)
«~~» или « - »	Исключает слово, перед которым стоит, из поиска
( )	Группирование слов или сложных запросов
"..."	Поиск точной фразы. Слова идут подряд в точной форме
"… * …"	Пропущено слово в цитате
… && …	Логическое И (в пределах документа). Слова в пределах одного документа
… << …	Неранжирующее "и": выражение после оператора не влияет на позицию документа в выдаче. Будут показаны документы, в которых есть слова, которые стоят до и после

	оператора, но слова после оператора, справа, не будут принимать участие в ранжировании
«Слово 1» /x «слово 2»	«x» – количество слов от «Слова 1», с учетом самого слова в любую сторону (то есть между заданными словами может встречаться x-1 слово)
«Слово 1» /+x «Слово 1»	Расстояние в пределах x-1 слов в прямом порядке
«Слово 1» /(-y +x) «Слово 2»	Расстояние от y слов в обратном порядке до x-1 слов в прямом
!«Слово»	Позволяет найти слова в соответствии с заглавной буквой
«слово1» && /x «Слово 2»	«x» – количество предложений между словами в любую сторону
!! «Слово»	Словарная форма слова
title:	Поиск по заголовкам документов
url:	Поиск по URL
inurl:	Поиск с учетом фрагмента URL
host:l	Поиск по хосту
rhost:	Поиск по хосту в обратной записи
site:http://www. … . …	Поиск по всем поддоменам и страницам заданного сайта
mime: «расширение»	Поиск по одному типу файлов
lang:«указание языка в международной транслитерации»	Поиск с ограничением по языку
domain:«указание доменной зоны»	Поиск с ограничением по домену
date:ГГММДД	Поиск с ограничением по дате
date: ГГММДД.. ГГММДД, date:> ГГММДД	Поиск с ограничением по интервалу дат

таблица 1

Синтаксис языковых запросов Google

Синтаксис	**Значение оператора**
+ (AND)	Обязательное наличие слова в найденном документе
- (NONE)	Исключает слово, перед которым стоит, из поиска
OR	Логическое ИЛИ
«…»	Поиск точной фразы. Слова идут подряд в точной форме
~	Поиск с учетом синонимов. Англоязычная вариация. ~hardware
.. (две точки)	Поиск с учетом диапазона чисел. Например: война 1900..1990

site:	Поиск по всем поддоменам и страницам заданного сайта
[#]…[#]	Поиск с числами с указанием пределов. В том числе и дат
filetype:	Поиск по типу документов
date:	Поиск с ограничением по дате
link:	Ссылка на интернет-ресурс

таблица 2

При работе с информацией необходимо помнить, что:

– информация, расположенная на сайтах, не статична, она постоянно изменяется, поэтому при фиксации такой информации обязательно фиксируется время работы и часовой пояс;

– ссылки на ресурсы, содержащие автоматический переход, с технической точки зрения аналогичны самому ресурсу (на ресурсах социальных сетей расположены, например, ссылки на видео экстремистской направленности, а не само видео);

– для гарантированного поиска информации, содержащейся в федеральном списке экстремистских материалов, целесообразно использовать базы значений хеш-функций этой информации;

– при определении данных об источниках, которые участвуют в распространении информации, устанавливаются учётные данные программно-аппаратной части, а не личность пользователя;

– при изъятии информации с серверов передачи и хранения данных изымается только необходимая информация, а не дисковый массив.

Самостоятельный поиск криминалистически значимой информации в Интернете зачастую затруднен отсутствием у следователя с специальных знаний в этой области. Особенно когда речь идет о непосредственном наблюдении за закрытыми для общего доступа местами общения правонарушителей путем осуществления интернет-мониторинга. Он предполагает изучение сообщений, публикуемых в соответствующих чатах, конференциях, на форумах, и обеспечивает возможность получать сведения о намерениях участников преступных формирований, устанавливать их связи между собой, узнавать

детали замышляемых деяний, выявлять признанных лидеров, следить за их перемещениями, вести подбор лиц для привлечения к сотрудничеству и т.д.

Участие специалиста в решении таких задач обеспечивает более широкий охват интернет-ресурсов и ускоряет деятельность. В целом роль специалиста для обнаружения и фиксации доказательств в компьютерных сетях шире. Она определяется спецификой хранения, обработки и передачи информации. От специалиста требуются знания именно в технической области, и привлекать такого специалиста необходимо на всех этапах жизненного цикла информации.

При обнаружении и фиксации доказательственной информации следует учитывать технические особенности компьютерных сетей, связанные с хранением, обработкой и передачей информации. Выделяют «открытые» сетевые ресурсы Интернета и «закрытые», куда относят пиринговые сети P2P и сети I2P – Invisible Internet Project (проект «невидимый интернет»), по сути являющийся зашифрованной анонимной сетью.

Самыми известными представителями P2P – сетей являются файлообменники, BitTorrent-трекеры и DirectConnect (DC++) хабы. Обе сети предназначены для обмена большими объёмами информации, как правило, это аудио и аудиовизуальная информация (фонограммы и фильмы). Следует знать, что сети DC популярны в пределах сети определённого провайдера (локальной сети провайдера) и требуют предоставления открытого ресурса на компьютере пользователя, подключившегося к сети DC++. Эти сети могут служить для относительно скрытного распространения большого объёма информации криминальной направленности.

Специалист фиксирует информацию о сетевых ресурсах, с которых производится обмен информацией, при этом учитывается, что файлы хранятся на компьютерах пользователей, а сервер осуществляет координацию работы сети. Так как на сервере хранятся IP-адреса и порты клиентов, то при доступе к данному серверу возможно определить источники, которые участвуют в распространении информации. Кроме того, специалист участвует в качестве консультанта для разъяснения терминов и действий пользователей.

Ниже приведено изображение программы yTorrent с указанием IP-адресов участников скачивания-раздачи (пиров) (рисунок 1).

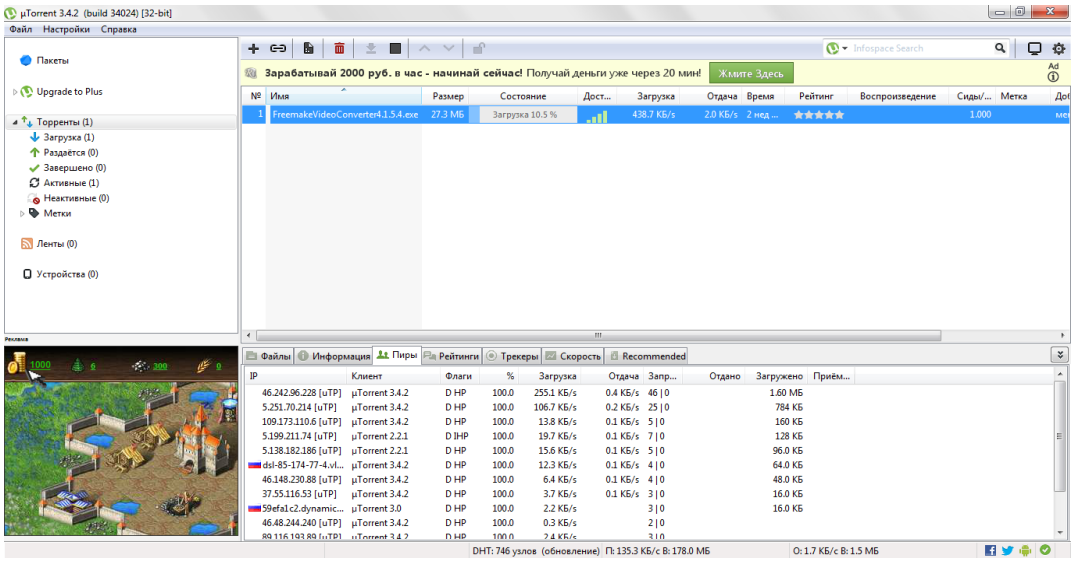

рисунок 1

I2P – это сеть внутри сети, анонимная оверлейная сеть. Она позволяет защитить передачу данных от внешнего наблюдения, в том числе от наблюдения провайдера, так как передаваемая информация и адреса сети шифруются. В качестве адреса (I2P-адрес) используется 32-байтный SHA-256 хеш от идентификатора. Информация, передаваемая по данной сети, провайдером не отслеживается, провайдер фиксирует активность участника как обмен зашифрованными пакетами с различными бессистемными адресами. Ниже приведено изображение сайта сети I2P (рисунок 2).

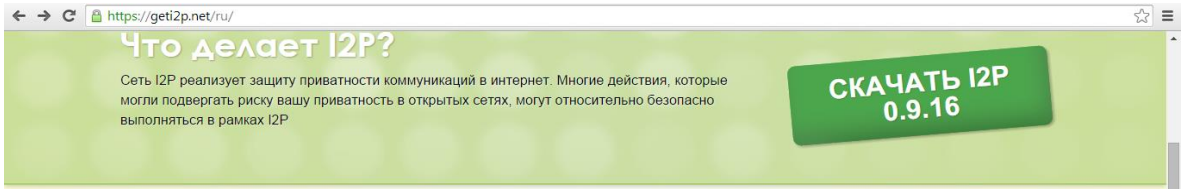

рисунок 2

В сети I2P реализованы следующие функции:

– электронная почта;

– Web browsing: анонимные веб-сайты, шлюзы в открытый Интернет и из него;

– блоги и форумы;

– встроенный анонимный веб-сервер;

– чаты и IRC-клиенты;

– файлообмен: ED2K и Gnutella, встроенный BitTorrent;

–распределённое хранение файлов.

Ниже приведено изображение консоли I2P-роутера (рисунок 3).

рисунок 3

Данные сети могут служить для скрытного распространения информации криминальной направленности, например скрытого обмена сообщениями.

Специалистов при работе с I2P -сетями привлекают в качестве консультанта для разъяснения терминов и действий пользователей и для определения источников передачи информации и перехвата сообщений. Для этих целей специалист использует известные уязвимости I2P- сетей: подмена узлов; перехват тоннеля; атака методом исключения; перехват ключа шифрования.

При работе с информацией, расположенной на открытых сетевых ресурсах, интернет-специалистов привлекают для выявления интересующей информации, определения данных об источниках, которые участвуют в распространении информации, и фиксации выявленной информации; в качестве консультанта.

Анкетирование следователей, расследующих дела о дорожно-транспортных преступлениях, показало, что ресурсы сети Интернет при расследовании используются преимущественно для размещения объявлений о поиске очевидцев происшествия, розыске скрывшихся с места происшествия транспортных средств или водителей. Данные объявления размещаются на

сайтах органов внутренних дел либо электронных версиях региональных СМИ.

Однако это лишь одно направление использования информационных ресурсов сети Интернет. Широкое распространение автомобильных видеорегистраторов повлекло появление в сети Интернет огромного количества видеозаписей дорожно-транспортных происшествий, выкладываемых в сеть очевидцами происшествия либо его участниками. Накоплению видеозаписей дорожно-транспортных происшествий способствует и большое количество камер видеонаблюдения и видеомониторинга. Видеоролики часто выкладываются в социальных сетях, а также на соответствующих тематических сайтах и форумах. Распространение получили и веб-камеры, устанавливаемые как различными организациями, так и физическими лицами с целью мониторинга дорожной ситуации на наиболее оживленных участках автодорог. Данные веб-камеры в режиме on-line транслируют изображение проезжей части и позволяют оценить загруженность дороги и выбрать наиболее оптимальный маршрут движения[8]. Соответственно, должный анализ содержания этих сетевых ресурсов может позволить получить объективную информацию о событии и механизме происшествия, его участниках, выявить свидетелей, очевидцев дорожно-транспортного происшествия. Большинство из этих возможностей уже давно используются рядом тематических интернет-сайтов, предлагающих как на коммерческой основе, так и бесплатно услуги водителям, ставшим участниками дорожно-транспортных происшествий, по поиску и представлению видеозаписей дорожно-транспортных происшествий, а также по размещению объявлений о поиске свидетелей, очевидцев происшествия[9].

Сама видеозапись, содержащаяся на каком-либо сайте, не может служить самостоятельным доказательством, поскольку неизвестен источник её происхождения и, следовательно, отсутствует такое важное свойство

[8] Например: интернет ресурс Яндекс имеет сотни видеокамер на автодорогах г. Москвы и других крупных городов. (URL: http://maps.yandex.ru) Сайт «Город из окна», объединяющий пользователей, установивших веб-камеры с видом на автодорогу в своих квартирах (URL: http://www.probkiizokna.ru)

[9] Например: интернет-сайты: Видел ДТП URL: http://виделдтп.рф; STOP! Не гони URL: http://www.stopnegoni.ru; DTP36.RU, URL: http://dtp36.ru и др.

доказательства, как достоверность. Для того чтобы придать ей статус доказательства, она должна быть не только соответствующим образом изъята и приобщена к материалам уголовного дела, но также должен быть установлен субъект, ее разместивший.

Чтобы установить пользователя того или иного аккаунта в социальной сети или разместившего интересующий нас контент, необходимо обладать информацией о его IP-адресе. Искомая информация может быть предоставлена непосредственно владельцами того интернет-ресурса, которым разыскиваемый абонент пользуется.

Знание IP-адреса пользователя позволяет установить город и страну проживания субъекта, а также получить информацию о его провайдере. В свою очередь провайдер уже имеет данные о фактическом местоположении пользователя проводного Интернета или о лице, которое приобрело SIM-карту.

Для получения сведений об IP-адресе следователю в соответствии с ч. 4 ст. 21 УПК РФ необходимо направить запрос руководству компании – владельцу социальной сети с просьбой предоставить используемый IP-адрес и время выхода в сеть конкретного субъекта. Время выхода в сеть позволит индивидуализировать разыскиваемое лицо в случае использования им динамического IP-адреса.

Для установления провайдера, предоставившего пользователю возможность выхода в Интернет, необходимо использовать базу данных IP-адресов интернет-провайдеров, размещенную в открытом доступе на интернет-ресурсе http://www.2ip.ru.

После установления провайдера ему необходимо направить запрос о предоставлении регистрационных данных пользователя, которому в конкретное время присваивался конкретный IP-адрес. В запросе рекомендуется также предоставлять информацию и о посещаемых искомым субъектом в указываемое время интернет-ресурсах. Это позволит индивидуализировать пользователя в случае предоставления интернет-провайдером услуг связи нескольким пользователям через единый узел связи под идентичным IP-адресом (преимущественно встречается при предоставлении услуг GPRS-связи сотовыми компаниями). Срок хранения информации о пользователях

провайдерами в соответствии со ст. 10.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» составляет шесть месяцев.

Важным источником доказательственной и ориентирующей информации может являться содержание электронной переписки фигурантов дела, ведущейся с использованием различных почтовых интернет-сервисов.

Владелец почтового аккаунта может вести активную переписку с иными участниками дела, передавать разного рода и степени важности документы, отправлять аудио- и видеофайлы переговоров, а также файлы, несущие разного рода смысловую нагрузку.

Существенным недостатком электронной почты с позиции правоохранительной деятельности является то, что при прохождении регистрации для получения почтового ящика пользователь, вводя свои персональные данные (идентификационные данные), может ввести любые сведения, даже не принадлежащие ему. Это в значительной степени затрудняет действия по установлению принадлежности конкретного почтового ящика тому или иному реальному субъекту.

Для получения доступа к электронной почтовой переписке следователь с согласия руководителя следственного органа возбуждает ходатайство перед судом о производстве выемки почтовой корреспонденции с электронного ресурса в соответствии со ст. 38, ч. 1 ст. 165, ч. 1, 2, 4 ст. 182 и ст. 183 УПК РФ.

В результате проведения выемки данной электронной информации следователем будут получены:

– регистрационные данные абонента почтового ресурса;

– электронный носитель с базой данных почтового ресурса, на котором происходила выемка электронной почтовой корреспонденции.

Полученные данные, изъятые следователем в ходе выемки на почтовом ресурсе, в порядке ст. 164, ч. 1 ст. 176, ч. 1–4 и 6 ст. 177 УПК РФ следует осмотреть в целях обнаружения следов преступления и выяснения обстоятельств, имеющих значение для раскрытия и расследования преступления.

В случаях, когда доказательственной является информация, хранящаяся на носителях, необходимо оценить возможность ее фиксации без изъятия электронных носителей и компьютерной техники.

Копирование как разновидность предметной формы фиксации доказательственной информации в деятельности по собиранию доказательств рассматривается как альтернативный метод изъятию предмета в натуре и его консервации. При этом предпочтительным методом предметной формы признается изъятие. Устоявшиеся представления о целесообразности изъятия носителя следа при производстве следственных и иных действий усваивается будущими юристами в период изучения тем криминалистической техники и тактики. В основе такого рода рекомендации по работе с «традиционными» следами в криминалистике лежит ряд вполне обоснованных утверждений:

– изъятие сводит к минимуму потери доказательственной информации, неизбежные при копировании, получении слепков и применении других приемов фиксации;

– при изъятии обеспечивается возможность непосредственного восприятия участниками процесса изъятого предмета, что исключает сомнения, могущие возникнуть при восприятии производных от него объектов;

– изъятием создаются условия для более полного исследования содержащейся в предмете информации, которая могла быть проигнорирована при его непосредственном обнаружении, а также сохраняется возможность получения копий предмета, если имеется возможность многократного копирования[10].

Сейчас уже ни у кого не вызывает резко отрицательного отношения использование в криминалистике и практике расследования терминов «виртуальный след» и «электронный цифровой объект». Сущность данных понятий имеет конкретное содержание и теоретически обоснована[11].

С учетом особенностей обращения информации в электронном виде формируются новые представления о формах, методах и средствах её фиксации

[10] Белкин Р.С. Курс криминалистики: В 3 т. – М., 1997. – Т. 2. – С. 59-62.

[11] Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе: монография. – М.: Юрлитинформ, – 2012. – С. 64.

в уголовном судопроизводстве. Цифровой вид записи информации позволяет без потерь криминалистически значимых сведений копировать различные цифровые объекты. При этом при перезаписи ни форма, ни строение вещества, из которого состоят носители компьютерной информации, не претерпевают никаких существенных изменений, а получаемые при копировании цифровых объектов вторая, третья и другие копии в информационно-содержательном плане абсолютно идентичны своему исходному варианту/

В Уголовно-процессуальном кодексе нет прямых ограничений на использование в качестве доказательств электронных носителей с записью копий файлов, имеющих доказательственное значение. Однако существует ряд факторов, значительно затрудняющих использование соответствующих копий в уголовном судопроизводстве. Одним из них является преобладающее до сих пор в среде юристов настороженное отношение к «электронным доказательствам». Это связано с достаточно скудными представлениями большинства гуманитариев об информационных технологиях и массовой убежденностью, что данные источники сведений легко фальсифицируются, а факт внесения изменения в содержание информации выявить почти невозможно. В связи с этим сформировалась определенная практика работы с «виртуальными следами». При производстве следственных действий следователи и дознаватели стараются изъять все возможные объекты, на которых, по их мнению, могут содержаться файлы, имеющие значение для расследования преступления. Тем самым они якобы предотвращают уничтожение информации и страхуются от возникновения в дальнейшем сомнений в достоверности полученных доказательств, так как получили первоисточник сведений, имеющих доказательственное значение. Однако изъятие предмета в натуре и его консервация является далеко не единственной формой фиксации доказательственной информации, а в ряде случаев с учетом закономерностей механизма следообразования на носителях электронной информации вообще неприемлема. В частности, достаточно сложно зафиксировать сведения, хранящиеся на НЖМД серверов, путем их изъятия.

Современные технологии, применяющиеся для хранения и обработки больших массивов данных, подразумевают такую архитектуру совокупности серверов как отдельных средств компьютерной техники, в том числе находящихся на большом расстоянии друг от друга, при которой они работают как единое хранилище информации. Физическое изъятие отдельных устройств или какой-то их совокупности может привести к невозможности восстановления интересующих следствие данных. Причины этого можно по аналогии объяснить на примере вскрытия жесткого диска компьютера и извлечения из него отдельных магнитных дисков. Физически информация в таком случае останется записанной на дисках, но использовать её будет невозможно.

Фактически только копирование как способ фиксации доказательственной информации может быть применено в отношении данных, хранящихся в облаке или на серверах компаний, представляющих услуги хранения и размещения медиаконтента (YouTube, Вконтакте и т.п.)

В полной мере реализации на практике возможностей копирования для фиксации доказательственной информации, хранящейся на ресурсах сети Интернет, при производстве следственного осмотра мешает устоявшаяся практика работы с электронными доказательствами. Наиболее популярным у следователей способом собирания таких доказательств остается производство выемки носителя с интересующими данными у владельца сайта или субъекта, предоставляющего услуги хостинга. Статья 183 УПК РФ в качестве основания производства выемки закрепляет необходимость изъятия определенных предметов и документов, имеющих значение для уголовного дела, если точно известно, где и у кого они находятся. Норма данной статьи, регламентирующая порядок участия специалиста при производстве выемки, предусматривает обязательное его приглашение при изъятии электронных носителей информации. Такие законодательные формулировки в значительной мере ограничивают возможность использования выемки для фиксации доказательственной информации. Копирование интересующей информации с носителя в рамках выемки без изъятия каких-либо объектов не допускается. Учитывая это,

следователи в бесконфликтных ситуациях заранее просят владельца сайта скопировать интересующие их файлы на другие носители (CD, DVD), а затем проводят выемку и изымают электронный носитель с копированными файлами. Такой путь получения доказательств трудно назвать допустимым. Прежде всего теряется возможность процессуального удостоверения факта появления копии информации, имеющей доказательственное значение. Не исключается возможность манипуляции с файлами лицами, которые будут производить копирование, если об их заинтересованности в исходе расследования следователю неизвестно. Ошибки в выборе метода копирования, объеме копируемой информации лицом, не имеющем специальных знаний в этой области, могут вообще исключить возможность использования полученных данных в качестве доказательств или снизить возможность дальнейшего экспертного исследования видеозаписи. Кроме того, такой способ собирания доказательств требует значительного количества времени, особенно если владелец сетевого ресурса находится за пределами России.

Процедура копирования информации в процессе следственного действия должна позволять решать задачи обеспечения достоверности сведений и их неизменности в процессе хранения. Фиксация источника копирования информации должна обязательно осуществляться в протоколе следственного действия.

Для того чтобы размещенные в сети Интернет видеоролики, тексты или аудиозаписи стали доказательством, необходимо их зафиксировать с учетом рекомендаций криминалистической тактики.

Если интересующее видео размещено на страничке пользователя социальной сети или каком-либо сайте, то необходимо осмотреть данный сайт или страничку. Осмотр может быть проведен в кабинете следователя с использованием его рабочего компьютера. В протоколе осмотра описывается внешний вид сайта и все действия, выполняемые следователем при переходе по ссылкам и пунктам меню. Необходимо учитывать время осмотра (т.к. информация на сайте динамическая и может постоянно изменяться), т.е. каждое действие по фиксации информации обязательно должно иметь привязку ко

времени. Нужно зафиксировать и указать в протоколе часовой пояс или время UTC Всеми́рное координи́рованное вре́мя (англ. Coordinated Universal Time, фр. Temps Universel Coordonné; UTC). Указывается адрес каждого окна сайта (берется из заголовка строки браузера). Для определения IP-адреса сайта можно воспользоваться специальным интернет-сервисом, который по доменному имени укажет IP-адреса, например ресурс http://ip-whois.net/website_ip.php. Страницы сайта копируются с помощью штатных средств интернет-браузеров, (меню «Сохранить страницу как»), или используют специализированное программное обеспечение для копирования всего содержимого сайта. Специальные программы применяются и для копирования видеороликов с YouTube. Такие программы свободно распространяются, имеют небольшой размер, и их легко найти в Интернете. Например, бесплатная программа HTTrack, страница https://www.httrack.com/.

В ряде случаев достаточно сделать скриншот страницы.

В протоколе обязательно необходимо указать технические средства (компьютер) и программное обеспечение, которые применялись при осмотре и копировании файлов. Скопированные файлы записываются на неперезаписываемый носитель и оформляются в качестве приложения к протоколу осмотра. Следует помнить, что на страницах социальных сетей и сайтах видеоролики обычно не хранятся. На них размещаются только ссылки для просмотра или скачивания. Сами ролики хранятся на серверах компаний, предоставляющих соответствующие услуги. Однако в правовом понимании размещение ссылок на ресурсе конкретного пользователя необходимо рассматривать как размещение соответствующих файлов, т.к. их активация приводит к получению необходимой информации.

Гарантом достоверности происхождения скопированной информации является участие при производстве следственного действия понятых. При этом важно, чтобы они понимали суть производимых действий, т.е. на языке современного обывателя были «продвинутыми пользователями» компьютерной техники. Использование технических средств фиксации хода и результата

следственного действия взамен понятых возможно в случаях, предусмотренных ст. 170 УПК РФ, но использование видеозаписи в этом случае менее эффективно, чем участие понятых. Применение специальных технических средств и программного обеспечения для копирования информации является обязательным. В настоящее время технико-криминалистическое обеспечение правоохранительных органов средствами копирования информации в электронном виде сконцентрировано на разработке и внедрении аппаратно-программных комплексов, использующихся для извлечения данных с электронных носителей информации. Среди них необходимо выделить дубликаторы, применяемые для копирования компьютерных носителей информации, имеющие возможность подключения через распространенные в настоящее время интерфейсы НЖМД и различных флэш-носителей, а также средства для клонирования памяти мобильных средств сотовой связи и других носимых гаджетов. Использование специальных программ и аппаратно-программных комплексов значительно упрощает работу следователя, так как в них автоматизированы наиболее типичные действия при производстве следственных действий в отношении данных в электронном виде и реализованы функции решения задач обеспечения достоверности полученных копий.

Решение вопроса о комплексном программно-техническом обеспечении копирования данных с удаленных ресурсов решается не так эффективно. Авторам неизвестны специально разработанные средства, которые бы непосредственно предназначались для копирования криминалистически значимой информации с удаленных открытых ресурсов Интернета в рамках производства следственных действий. Однако в большинстве случаев необходимости копирования электронной информации это можно осуществить путем использования распространенного компьютерного оборудования и программных средств. Производство следственного действия, связанного с копированием данных с удаленных источников, целесообразно осуществлять с участием специалиста, однако реализация криминалистических рекомендаций

позволяет осуществить его самостоятельно лицом, производящим следственное действие и имеющим навыки собирания электронных доказательств.

Как было частично сказано выше, для копирования данных с удаленных источников следователю необходимо иметь компьютер, подключенный к сети Интернет, с приводом для записи CD-DVD дисков в том случае, если осмотр сайта или иного ресурса в сети происходит с рабочего места следователя. Когда же осмотр удаленного ресурса является стадией осмотра места происшествия (например, в ситуации, если в рамках осмотра на рабочем месте подозреваемого обнаруживается открытая сессия обмена данными с удаленным закрытым (облачным) хранилищем), бывает достаточно одного внешнего привода, подключаемого через USB-интерфейс. Также необходимо достаточное количество оптических дисков или иных электронных носителей информации, на которые предполагается копирование. Необходимое программное обеспечение включает в себя носители с portable-версиями программ, использующихся для копирования сайтов, скачивания файлов со специализированных ресурсов, на которых они выложены только для просмотра (например, с YouTube), для создания скриншотов или записи в видеофайл событий, демонстрируемых на мониторе компьютера, создания архивов скопированной совокупности файлов и подсчета хеш-сумм копируемой информации. Предназначение большинства перечисленных объектов для современных пользователей компьютерной техники не требует разъяснения.

Все из перечисленных программ представлены в Интернете для свободного скачивания и использования различными разработчиками. Программы для копирования сайтов предназначены, прежде всего, для обеспечения возможностей пользователей знакомиться с содержимым сайта в автономном режиме (без подключения к Интернету) после его скачивания на электронный носитель компьютера или съемный носитель. В отличие от использования функции браузеров «Сохранить как» использование таких программ позволяет сохранить структуру сайта с возможностью

функционирования внутренних гиперссылок. Использование таких программ удобно для оперативного копирования фишинговых сайтов: их внешнего вида, внутренней структуры и контента.

Программы для скачивания медиафайлов, размещенных для просмотра, обеспечивают их копирование даже в случае отсутствия такой возможности, реализованной на сайте. Эти программы могут быть в виде плагинов к браузерам или как отдельные программные продукты. Их использование уместно прежде всего для копирования различных видеороликов с записями преступных действий, которые выкладывают очевидцы на сайты (видеохостинги).

Возможность снятия скриншотов обеспечивает запись файлов с изображениями на мониторе компьютера в определенные моменты времени. Данная функция может быть реализована средствами операционной системы.

Клавиша на компьютерных клавиатурах PrtScr или Print Scrn обычно расположена в секции с клавишами Break и Scroll Lock. Print Screen находится на одной кнопке с SysRq. При ее нажатии в Windows изображение монитора копируется в буфер обмена и требует дальнейшего сохранения путем использования программ графических редакторов. Более удобны в использовании специальные программы для снятия скриншотов. При их применении обычно можно настроить параметры автоматического снятия скриншотов через определенные промежутки времени, выбрать формат файлов и адрес для их сохранения. Более широкие возможности для фиксации хода и результатов следственного действия представляют программы, осуществляющие запись изображения монитора в видеофайлы. Их использованием можно заменить обычную видеосъемку следственного действия в части осмотра содержимого удаленного ресурса.

Программы для определения хеш-суммы копируемой информации используются для её аутентификации, т.е. установления и подтверждения неизменности информации. Данный термин в области информационных технологий применяется для обозначения процедур проверки подлинности пользователя путём сравнения введённого им пароля с паролем в базе данных

пользователей, подтверждения подлинности электронного письма путём проверки цифровой подписи по ключу проверки подписи отправителя; проверки контрольной суммы файла на соответствие сумме, заявленной автором этого файла.

Чтобы предотвратить сомнения в том, что в процессе копирования информации или при ее хранении могли быть внесены изменения, необходимо вычислить контрольную сумму или хеш-сумму (данные термины являются синонимами) копируемых файлов или копируемых разделов электронного носителя информации до их копирования и после. Контрольные суммы необходимо переписать в протокол следственного действия.

Термин «хеширование» в сфере информационных технологий используется для обозначения процесса преобразования по определённому алгоритму входного массива данных произвольной длины в выходную битовую строку фиксированной длины. Такие преобразования также называются хеш-функциями или функциями свёртки, а их результаты называют хешем, хеш-кодом или сводкой сообщения. Хеширование применяется для построения ассоциативных массивов, поиска дубликатов в сериях наборов данных, построения достаточно уникальных идентификаторов для наборов данных, контрольного суммирования с целью обнаружения случайных или намеренных ошибок при хранении или передаче информации, для хранения паролей в системах защиты, при выработке электронной подписи. Значение хеширования для аутентификации при копировании и хранении информации заключается в том, что однозначного соответствия между исходными данными и хеш-кодом нет в силу того, что количество значений хеш-функций меньше, чем число вариантов значений входного массива. Необходимо также понимать, что существует множество массивов с разным содержимым, но дающих одинаковые хеш-коды – так называемые коллизии. Вероятность возникновения коллизий играет немаловажную роль в оценке качества хеш-функций. Существует множество алгоритмов хеширования с различными свойствами (разрядность, вычислительная сложность, криптостойкость и т.п.). Выбор той или иной хеш-функции определяется спецификой решаемой задачи.

Простейшими примерами хеш-функций могут служить контрольная сумма или CRC. При выборе программ для вычисления хеш-суммы копируемой информации необходимо учитывать, что «хорошая» хеш-функция должна удовлетворять двум свойствам: быстро вычисляться и минимизировать количество коллизий/ Для решения обозначенных нами задач целесообразно применять программы, реализующие криптографические хеш-функции, т.е. стойкие к коллизиям, применяемые в криптографии. Примером такой функции является алгоритм «Стрибог», утвержденный ГОСТ Р 34.11-2012, использующийся для хеширования при формировании цифровой подписи.

Если лицо, производящее следственное действие, имеет электронную подпись, т.е. соответствующий набор программ, то для определения хеш-суммы копируемых данных целесообразно использовать сертифицированную программу, входящую в данный набор. Сложность заключается в том, что подавляющее большинство сотрудников правоохранительных органов не обеспечены электронной цифровой подписью. В таком случае уместно использовать иные программы хеширования. Авторам неизвестны свободные программные продукты, реализующие алгоритм «Стрибог», поэтому в качестве рекомендации остановимся на программах, реализующих наиболее распространенный алгоритм хеширования, – MD5. Примером таких программ являются md5summer и HashTab. Определение хеша по данному алгоритму реализовано и в достаточно популярной у пользователей файловой оболочке Total Commander.

Хеширование скопированных файлов и фиксация кода в протокол следственного действия обеспечивает возможность проверки их подлинности в любой момент времени. Вычисление хеша файлов, скопированных с пиринговых файлообменных сетей или ftp-серверов, позволяет также установить их аутентичность файлам, размещенным на соответствующих ресурсах, если лицо, их разместившее, указало значение функции в описании файлов.

Запись скопированных файлов мы рекомендуем осуществлять только на неперезаписываемый носитель, который будет прилагаться к протоколу

следственного действия без создания мультисессии. Чтобы снизить риск случайного или умышленного изменения файлов в процессе их хранения или работы с ними, мы рекомендуем записать их единым файлом архива, предварительно установив хеш каждого файла и хеш архива. Данные внести в протокол следственного действия.

Использование свободных программных продуктов, не сертифицированных ФСТЭК России, не противоречит нормам УПК РФ. Возникновение возможных сомнений в том, что такая программа может скрытно для пользователя реализовать вредоносные функции, в том числе изменить копируемые данные, устраняется путем приложения к протоколу следственного действия неперезаписываемого оптического диска или иного носителя, на которых записаны portable-версии использованных свободных программ, с которых они запускались. Если в процессе дальнейшего производства по делу будет установлено противоречие доказательств, его всегда можно будет устранить путем экспертизы вызвавших сомнение программ.

Таким образом, при поиске и фиксации криминалистически значимой информации на ресурсах сети Интернет необходимо учитывать тактические рекомендации:

– субъектами поиска криминалистически значимой информации в сети Интернет могут выступать сотрудники оперативных подразделений органов внутренних дел, следователи и дознаватели;

– поиск по информационным ресурсам Интернета может быть реализован через различного рода поисковые системы (Google, Yandex, Rambler и т.п.), использующие производительные алгоритмы обнаружения информации по заданным реквизитам;

– повышение эффективности поиска в Интернете предполагает применение контент-анализа, который представляет собой формализованный аналитический метод исследования содержания документов в целях выявления и измерения характеристик социальных явлений, получивших в них отражение;

– наиболее широкие возможности контент-анализа социальных сетей представляет использование программного обеспечения UFED, Мобильный криминалист, XRY, U2;

– участие специалиста в решении поисковых задач обеспечивает более широкий охват интернет-ресурсов и ускоряет соответствующую деятельность;

– выявление и сбор данных специалистом включает проведение аналитической и компьютерной разведок, основной задачей которых будет поиск информации;

– важным источником доказательственной и ориентирующей информации может являться содержание электронной переписки фигурантов дела, ведущейся с использованием различных почтовых интернет-сервисов. Порядок получения доступа к переписке включает в себя действия по установлению адресов почтовых ящиков, используемых преступником, получения разрешения суда на ее выемку и действия по изъятию и осмотру носителя с электронной корреспонденцией;

– фиксация доказательственной информации, хранящейся на ресурсах Интернета, осуществляется посредством протоколирования следственного действия, изъятием носителя информации и копированием данных;

– в протоколе обязательно необходимо указать признаки интернет-ресурса, произведенные действия, технические средства (компьютер) и программное обеспечение, которые применялись при осмотре и копировании файлов. Скопированные файлы записываются на неперезаписываемый носитель и оформляются в качестве приложения к протоколу осмотра;

– программное обеспечение при осуществлении фиксации информации с удаленных ресурсов при производстве следственного осмотра включает в себя носители с portable-версиями программ, использующихся для копирования сайтов, скачивания файлов со специализированных ресурсов, на которых они выложены только для просмотра (например, с YouTube), для создания скриншотов или записи в видеофайл событий, демонстрируемых на мониторе компьютера, создания архивов скопированной совокупности файлов и подсчета хеш-сумм копируемой информации.

ЗАКЛЮЧЕНИЕ

В данной работе на основе анализа теоретических положений наук уголовного процесса и криминалистики, норм уголовно-процессуального права, правоприменительной практики и опыта деятельности правоохранительных органов предложены рекомендации по фиксации доказательственной информации, хранящейся на ресурсах Интернета. В частности, выделены условия, определяющие тактику и способы фиксации данных, разработаны рекомендации по поиску и фиксации криминалистически значимой информации, размещенной в сети Интернет, предложен порядок использования неспециализированного оборудования компьютерных программ для процессуального копирования криминалистически значимой информации с удаленных сетевых ресурсов.

Основными положениями и выводами в работе являются следующие:

– целесообразность использования в раскрытии и расследовании преступлений сведений, размещенных на ресурсах сети Интернет, обуславливается тем, что такого рода информация может существенно облегчить выбор направлений поисковой деятельности, а также планирование проведения оперативно-розыскных и следственных мероприятий; поиск информации на открытых ресурсах быстрее, а иногда и эффективнее, чем при добывании ее с помощью негласных мероприятий; в условиях дефицита времени такие источники являются единственным средством быстрого получения необходимой информации; зафиксированные сведения, содержащиеся на ресурсах Интернета, можно использовать для выявления иной криминалистически значимой информации, относящейся к расследуемому событию;

– наибольший объем значимой в раскрытии и расследовании информации, которая может использоваться в качестве доказательственной, содержат следующие интернет-ресурсы: электронная почта, социальные сети, видеохостинги, интернет-магазины, веб-форумы, ftp-серверы, пиринговые сети, облачные хранилища информации и чаты;

– факторами, определяющими способ и тактику фиксации доказательственной информации из сети, являются технические и программные особенности обращения информации на конкретных ресурсах и ее характер, правовые аспекты организации и функционирования ресурса, а также защиты информации, направления ее дальнейшего использования в расследовании преступлений, обеспечение своевременности фиксации данных;

– обеспечение достоверности и допустимости доказательств из сети Интернет при производстве следственных действий осуществляется в рамках комплексных подходов, сочетающих технические методы, делающие невозможным сам факт внесения изменений в фиксируемые данные, и тактические приемы производства следственных действий;

– субъектами поиска криминалистически значимой информации в сети Интернет могут выступать сотрудники оперативных подразделений органов внутренних дел, следователи и дознаватели;

– поиск по информационным ресурсам Интернета может быть реализован через различного рода поисковые системы (Google, Yandex, Rambler и т.п.), использующие производительные алгоритмы обнаружения информации по заданным реквизитам;

– участие специалиста в решении поисковых задач обеспечивает более широкий охват интернет-ресурсов и ускоряет соответствующую деятельность;

– важным источником доказательственной и ориентирующей информации может являться содержание электронной переписки участников дела, ведущейся с использованием различных почтовых интернет-сервисов. Порядок получения доступа к переписке включает в себя действия по установлению адресов почтовых ящиков, используемых преступником, получения разрешения суда на ее выемку и действия по изъятию и осмотру носителя с электронной корреспонденцией;

– фиксация доказательственной информации, хранящейся на ресурсах Интернета, осуществляется посредством протоколирования следственного действия, изъятием носителя информации и копированием данных;

– в протоколе обязательно необходимо указать признаки интернет-

ресурса, произведенные действия, технические средства (компьютер) и программное обеспечение, которые применялись при осмотре и копировании файлов. Скопированные файлы записываются на неперезаписываемый носитель и оформляются в качестве приложения к протоколу осмотра;

– программное обеспечение при осуществлении фиксации информации с удаленных ресурсов при производстве следственного осмотра включает в себя носители с portable-версиями программ, использующихся для копирования сайтов, скачивания файлов со специализированных ресурсов, на которых они выложены только для просмотра (например, с YouTube), для создания скриншотов или записи в видеофайл событий, демонстрируемых на мониторе компьютера, создания архивов скопированной совокупности файлов и подсчета хеш-сумм копируемой информации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе: монография / В.Ю. Агибалов. – М.: Юрлитинформ, 2012. – 152 с.
2. Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе: монография / В.Ю. Агибалов – М.: Юрлитинформ, – 2012. – С. 64.
3. Багмет А.М. Извлечение данных из электронных устройств как самостоятельное следственное действие / А.М. Багмет, С.Ю. Скобелин // Право и кибербезопасность. – 2013. – № 2. – С. 22–27.
4. Барабанов А.В. Формирование требований по безопасности информации к DLP-системам / А.В. Барабанов, М.И. Гришин, А.С. Марков, В.Л. Цирлов // Вопросы радиоэлектроники. – 2013. – № 2. – С. 67–76.
5. Белкин Р.С. Курс криминалистики: 3 т. / Р.С. Белкин. – М., 1997. – Т. 2. – С. 59–62.
6. Зуев С.В. Электронное копирование информации как самостоятельное следственное действие / С.В. Зуев, К.И. Сутягин // Следователь. – 2003. – № 4.
7. Ишин А.М. Современные проблемы использования сети Интернет в расследовании преступлений / А.М. Ишин // Вестник Балтийского федерального университета им. И. Канта. – 2013. – № 9. – С. 34.
8. Каспаров С. Проверка электронной почты сотрудников. Как контролировать переписку на законных основаниях / С. Каспаров // Петербуржский правовой портал. – URL: – http://ppt.ru/news/117831 (дата обращения: 06.06.2015).
9. Копланд против Соединенного Королевства (Copland v. United Kingdom): Постановление Европейского Суда по правам человека от 3 апреля 2007 года (жалоба № 62617/00) // Бюллетень Европейского Суда по правам человека. – 2007. – № 10.
10. Матвеев В.А. Состояние и перспективы развития индустрии информационной безопасности Российской Федерации в 2011 г. / В.А. Матвеев, Н.В. Медведев, И.И. Троицкий, В.Л. Цирлов // Вестник МГТУ им.

Н.Э. Баумана. Сер. «Приборостроение». Спецвыпуск «Технические средства и системы защиты информации». – М., 2011. – С. 3–6.

11. Мещеряков В.А. Понятие и виды следственного осмотра при расследовании преступлений в сфере использования информационно-коммуникационных технологий / В.А. Мещеряков // Библиотека криминалиста. – 2014. – № 5.

12. Мещеряков В.А. Цифровые (виртуальные) следы в уголовном процессе и криминалистике / В.А. Мещеряков // Воронежские криминалистические чтения: сб. науч. трудов / под ред. О.Я. Баева. – Воронеж, – 2008. – Вып. 9. – С. 221–233; Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе: монография / В.Ю. Агибалов – М.: Юрлитинформ, – 2012. – 152 с.

13. Например: интернет-ресурс Яндекс имеет сотни видеокамер на автодорогах г. Москвы и других крупных городов. – URL: http://maps.yandex.ru. Сайт «Город из окна», объединяющий пользователей, установивших веб-камеры с видом на автодорогу в своих квартирах. – URL: http://www.probkiizokna.ru.

14. Например: интернет-сайты: Видел ДТП. – URL: http://виделдтп.рф; STOP! Не гони. – URL: http://www.stopnegoni.ru; DTP36.RU. – URL: http://dtp36.ru и др.

15. Юзбекова И. Центробанк рекомендовал российским банкам следить за своими сотрудниками / И. Юзбекова, Т. Алешкина // РБК daily. – URL: http://rbcdaily.ru/media/ 562949991666877 (дата обращения: 06.06.2015).