УДК 343.985.7:343.132.1

Светлана Игоревна ЗЕМЦОВА,
старший преподаватель кафедры криминалистики Сибирского юридического института МВД России (г. Красноярск)
Zemsvetlana@mail.ru

Олег Александрович СУРОВ,
начальник кафедры криминалистики Сибирского юридического института МВД России (г. Красноярск), кандидат юридических наук, доцент
79835086432@yandex.ru

Павел Викторович ГАЛУШИН,
старший преподаватель кафедры информационно-правовых дисциплин и специальной техники Сибирского юридического института МВД России (г. Красноярск), кандидат технических наук
galushin@gmail.com

ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ АСПЕКТЫ ПРОИЗВОДСТВА ОСМОТРА КОМПЬЮТЕРА ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С НЕЗАКОННЫМ ОБОРОТОМ "ДИЗАЙНЕРСКИХ" НАРКОТИКОВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНТЕРНЕТ-МАГАЗИНОВ

ORGANIZATIONAL AND TACTICAL ASPECTS OF COMPUTER EXAMINATION PROCEDURE IN INVESTIGATION OF CRIMES INVOLVING ILLEGAL TRAFFICKING IN DESIGNER DRUGS AND COMMITTED BY USING ON-LINE STORES

В статье на основе изучения судебно-следственной практики формулируется алгоритм осмотра компьютера при расследовании преступлений, связанных с незаконным оборотом наркотиков, совершаемых с использованием интернет-магазинов. При этом наиболее детально описывается элемент алгоритма "исследование данных браузера". Кроме того в работе освещаются новые сложные схемы движения денежных средств с использованием QIWI ваучеров и криптовалюты Bitcoin при совершении наркопреступлений.

The algorithm of examination of a computer in the investigation of illegal drug trafficking crimes committed by using on-line stores is formulated in the article on the basis of studying of judicial and investigative practice. And at the same time such element of the algorithm as "examination of browser data" is described in details. Besides new complicated schemes of cash flow with using QIWI vouchers and Bitcoin cryptocurrency in commission of drug-related crimes are under consideration.

Ключевые слова: *следственный осмотр, компьютер, Интернет, наркотические средства, специалист, виртуальные следы.*

Keywords: *investigative examination, computer, Internet, drugs, expert, virtual traces.*

Сложившийся за два последних десятилетия высокий уровень наркотизации населения России остается прямой угрозой национальной безопасности и основным фактором подрыва демографического и социально-экономического потенциала страны. Наряду с глобальным трафиком афганского героина существенную угрозу обществу представляет захлестнувший Россию поток новых синтетических психоактивных веществ (стимуляторов амфетаминового ряда, синтетических анальгетиков, синтетических каннабиноидов группы JWH и др.). Они поступают из стран Юго-Восточной Азии, Нидерландов, Германии, Пакистана, Индии, Ирана.

С целью увеличения числа наркопотребителей участники наркобизнеса все активнее используют сеть Интернет, что позволяет не только применять повышенные меры конспирации, но и осуществлять оперативный поиск продавцов и покупателей. При этом указанная деятельность все чаще носит трансрегиональный и трансконтинентальный характер и выражается в функционировании интернет-магазинов.

Изменившиеся способы совершения преступления предполагают совершенствование тактики производства отдельных [2; 3; 4; 5] следственных действий, в том числе и следственного осмотра. Несмотря на то, что в значительном количестве диссертационных исследований, методических рекомендаций, пособий детально освещается тактика его производства, практически отсутствуют работы, раскрывающие специфику осмотра компьютера при расследовании преступлений рассматриваемой категории. А в единичных публикациях этот вопрос освещается лишь фрагментарно.

Вместе с тем именно компьютер выступает одним из средств совершения преступлений, связанных с незаконным оборотом наркотических средств, психотропных и сильнодействующих веществ, совершаемых с использованием информационно-телекоммуникационных сетей. Значимость информации, которая может быть при этом получена, сложно переоценить. Так, в процессе его производства могут быть обнаружены как материальные (следы пальцев рук, микрообъекты и т.д.), так и виртуальные (посещение сайтов с рекламой наркотиков, архив переписки пользователя, управление счетами электронных платежных систем и т.д.) следы, способствующие формированию полноценной доказательственной базы и изобличающие не только его пользователя, но и иных лиц, причастных к совершению преступления: курьеров, менеджеров по региону, кассиров, организаторов преступных групп.

Иллюстративным является следующий пример из судебно-следственной практики.

При производстве обследования жилища гр. Ш., выполнявшего в организованной преступной группе функции "склада-хранителя", были изъяты системный блок, монитор "PHILIPS", ноутбук "ASUS". В ходе следственного осмотра, произведенного с участием специалиста, на диске "С" была обнаружена папка "Ozon77777" с файлами, содержащими текстовые записи, представляющие переписку абонентов "Ozon77777", "Ellektra911" за период с 19 октября 2013 г. по 14 декабря 2013 г. В ходе расследования было установлено, что под логином "Ellektra911" выступала сама Ш. Логин "Ozon77777" принадлежал лицу, осуществлявшему в организованной преступной группе функции оператора. В результате изучения переписки было установлено, что оператор передавал Ш. партии наркотиков для дальнейшего сбыта, давал указания о производстве закладок с наркотиками, инструктировал Ш. о правилах безопасного осуществления преступной деятельности, а также требованиях к отчетности о количестве приготовленных закладок и массе реализуемых наркотиков. Ш., в свою очередь, сообщала оператору адреса и места нахождения приготовленных ею закладок с наркотиками, номера своих QIWI-кошельков для получения денежного вознаграждения – зарплаты от оператора за произведенную работу по сбыту наркотиков.

На ноутбуке "ASUS" также была обнаружена переписка с использованием программы "Brosix" между "Ellektra911" и

"Иван Иванов", а впоследствии "Ozon77777", состоящая в получении заданий по реализации наркотиков (уголовное дело №23224271 по обвинению Ш. в совершении преступлений, предусмотренных: ч. 3 ст. 30, пп. "а", "г" ч. 4 ст. 228.1 УК РФ, ч. 1 ст. 30, пп. "а", "г" ч. 4 ст. 228.1 УК РФ, ч. 3 ст. 30, пп. "а", "г" ч. 4 ст. 228.1 УК РФ, ч. 3 ст. 30, ч. 5 ст. 228.1 УК РФ, ч. 1 ст. 30, ч. 5 ст. 228.1 УК РФ, ч. 1 ст. 174.1 УК РФ, направлено заместителю прокурора г. Норильска 25 июня 2014 г.).

Представленный и множество других примеров судебно-следственной практики свидетельствуют, что персональный компьютер является важным источником криминалистически значимой информации, которую можно получить в том числе при производстве осмотра данного объекта. Оптимизации этого процесса, полагаем, будет способствовать разработанный нами ***алгоритм действий***[1], (здесь и далее выделено нами. – С.З., О.С., П.Г.) основой которого является традиционный подход, состоящий в выделении этапов: подготовительного, рабочего, заключительного.

Производство подготовительного этапа (как на стадии до выезда на место происшествия, так и по прибытии на него), как правило, сложности не представляет. Специфика стадии до выезда на место происшествия будет заключаться в приглашении специалиста. При этом следует помнить о том, что общего понятия "специалист по компьютерной технике" не существует; можно говорить лишь о специалисте, сведущем в конкретной области информационных технологий. [1] Так, специалист по операционной системе Windows не обязательно будет знаком с операционной системой Mac OS, а поэтому необходимый профиль знаний конкретного специалиста следует определять в зависимости от целей и задач осмотра с учетом первоначальных данных о характере преступления.

По прибытии на место происшествия необходимо определить границы осмотра, его "узлы" (места, где максимально может быть сконцентрирована следовая информация), ограничить доступ к средствам компьютерной техники и электропроводке.

Алгоритм действий на **рабочем этапе** более сложный. В связи с этим рассмотрим его более детально.

На статической стадии рассматриваемого этапа целесообразно:

1) установить местоположение стационарного или мобильного ПК *(к последним относятся ноутбуки, планшетные и карманные ПК)*. Это может быть сделано посредством описания его расположения с указанием расстояния до двух неподвижных ориентиров;

2) выявить индивидуальные признаки системного блока, монитора, клавиатуры, мыши и другого периферийного оборудования.

Осмотр ПК, впрочем, как и практически любого объекта, необходимо начать с его внешнего осмотра, указав размер, цвет, маркировочные обозначения, специальные знаки и наклейки, нанесенные на корпус и устройства, механические повреждения.

Если на момент осмотра компьютер оказался включен, необходимо изучить изображение на экране монитора, отразив сведения об этом в протоколе. При этом специалист-криминалист может оказать содействие следователю при фиксации данной информации при помощи фото или/и видеозаписи;

3) изучить внешние устройства, подключенные к ПК. Это могут быть клавиатура, компьютерная мышь, акустическая система, сканеры, копировально-множительная техника, роутер, модемы, внешние накопители информации (переносные жесткие диски, носители на основе флэш-памяти). Например, при наличии сканера можно предполагать наличие в

1 В данной статье авторами компьютер рассматривается как один из объектов осмотра места происшествия. Вместе с тем представленный алгоритм может быть использован при производстве осмотра предмета (ПК), а также обыска.

памяти компьютера графических файлов; а при наличии электронного ключа, устанавливаемого в USB-порт или последовательный порт, – наличие программных средств защиты информации и т.д.

Внешние устройства должны быть сфотографированы. Кроме этого в процессе осмотра может быть изготовлена и приобщена к протоколу схема расположения данных устройств.

На этой же стадии (статической) необходимо обратить внимание на компьютерную литературу, особенно технически сложную, поскольку это свидетельствует о высокой квалификации пользователя и возможном наличии средств для уничтожения информации.

Значительно более трудоемкой является **динамическая стадия рабочего этапа осмотра места происшествия**. При этом последовательность действий может быть следующей.

1. Применить криминалистические средства (лупа, дактилоскопические порошки и т.д.) для обнаружения на внешних устройствах, подключенных к ПК, материальной информации (следов пальцев рук, микрообъектов).

2. Изучить аппаратное содержимое ПК. В первую очередь необходимо обратить внимание на жесткий диск и сетевую карту. Обусловлено это тем, что именно на жестком диске хранится информация, которая в дальнейшем может быть исследована. Сетевые карты обладают уникальным номером (MAC-адресом), который используется интернет-провайдерами для идентификации своих клиентов. Остальное аппаратное обеспечение – процессор, материнская плата, оперативная память не сохраняют информацию при выключении питания компьютера и не имеют существенного значения для расследования. В протоколе осмотра необходимо указать производителя и серийный номер данных жесткого диска, сетевой и материнской платы.

3. Установить операционную систему. Она может быть опознана по характерному виду графического интерфейса и логотипам (MicrosoftWinodws:XP, Vista, 7, 8, 10; Mac OS, операционные системы семейства GNU/Linux и др.). Поскольку следователи (дознаватели) не всегда компетентны в этом вопросе, консультационную помощь может оказать специалист в области компьютерных технологий, которого, как мы уже отмечали, целесообразно привлечь к производству данного следственного действия.

4. Установить IP и физический адреса. IP-адрес присваивается интернет-провайдером и используется для идентификации компьютера в сети Интернет при передаче и приеме информации. Физический адрес (MAC-адрес) задается каждому устройству, предназначенному для работы в компьютерных сетях, на заводе-изготовителе. Он используется, например, интернет-провайдером для идентификации клиентов. Однако следует помнить, что физический адрес может быть подменен средствами операционной системы.

Установление IP- и MAC-адресов и сопоставление их с данными, полученными от провайдеров интернет-услуг и платежных систем, позволяет установить причастность пользователя (например, выполняющего функции оператора) к совершению преступления.

5. Изучить данные браузера.

В глобальной сети браузеры используют для запроса, обработки, манипулирования и отображения содержания веб-сайтов. Многие современные браузеры также могут использоваться для обмена файлами с серверами ftp, а также для непосредственного просмотра содержания файлов многих графических форматов (gif, jpeg, png, svg), аудиовидеоформатов (mp3, mpeg), текстовых форматов (pdf, djvu) и других файлов.

Браузеры распространяются, как правило, бесплатно. Потребителям браузер может быть поставлен в форме самостоятельного (автономного) приложения или в составе комплектного программного обеспечения. К примеру, браузер Internet Explorer поставляется в составе операционной системы Microsoft Windows; Mozilla Firefox – отдельно или в составе дистрибу-

тивов Linux (например, Ubuntu); Safari – в составе операционной системы Mac OS X и в качестве приложения для Microsoft Windows; Google Chrome, Opera и другие браузеры – как самостоятельные программы во множестве вариантов для различных операционных систем.

При осмотре браузера необходимо проявлять осторожность: не закрывать открытые вкладки (это может привести к прекращению сеанса работы с сервисом, требующим ввода пароля), переход по гиперссылкам осуществлять в режиме "открыть на новой вкладке".

Существенное значение может иметь информация, полученная при изучении *истории просмотра веб-страниц и закладок в браузере*. При этом особого внимания заслуживают:

1) социальные сети ("ВКонтакте", "Facebook", "Одноклассники" и т.д.).

Так, при расследовании уголовного дела по обвинению Ш. в совершении контрабанды сильнодействующих веществ был произведен следственный осмотр системного блока и монитора компьютера. Используя пароль и логин, предоставленный Ш., через браузер Google Chrome был осуществлен вход в социальную *сеть "ВКонтакте"*, где на странице пользователя "Мои сообщения" была обнаружена переписка между Б. и Ш, которая длилась с 19 марта 2013 г. по 20 марта 2013 г. При этом от имени Б. выступал оперуполномоченный отделения по контролю за легальным оборотом наркотиков управления ФСКН по Псковской области. Интернет-перепиской установлено, что Ш. в полном объеме имел представление о препаратах, оборот которых запрещен в Российской Федерации, понимал, что через Интернет заказал анаболические стероиды, которые содержат в составе сильнодействующие вещества, получил счет для оплаты, перевел оплату за заказанные препараты, получил трек-код посылки, которую отслеживал, после чего при поступлении посылки в отделение почтовой связи собирался ее получить (уголовное дело № 20132800125 по обвинению Ш. в совершении преступления, предусмотренного ч.1 ст. 226.1 УК РФ, направлено прокурору г. Пскова 22 мая 2013 г.);

2) информация с различных сайтов, которые посещал подозреваемый (обвиняемый):

– содержащая сведения об изготовлении наркотических средств (о химических реактивах, оборудовании, алгоритме действий и т.д.).

Так, А. и Г. по предварительному сговору на незаконное приобретение посредством сети Интернет с использованием браузера Opera через транспортную компанию ООО "...", расположенную в г. Новосибирске, и службу доставки "...", расположенную в этом же городе, заказали из ООО "..." и ЗАО "...", расположенных в г. Москве и г. Санкт-Петербурге, необходимые для изготовления наркотического средства "...", лабораторное оборудование и химические реактивы, которые доставили на квартиру А. После чего А. и Г., обладая познаниями в области химии и используя в качестве пособия статьи о химических реактивах, об изготовлении наркотического средства, опубликованные в сети Интернет, незаконно изготовили наркотическое средство "...". В дальнейшем А. и Г. неоднократно осуществляли сбыт наркотического средства (уголовное дело № 25718 по обвинению гр. А. в совершении преступлений, предусмотренных ч. 2 ст. 228, п. "г" ч. 3 ст. 228.1, п. "г" ст. 228.1, ст. 30, п. "г" ч. 3 ст. 228.1 УК РФ; гр. Г. в совершении преступлений, предусмотренных ч. 2 ст. 228, ч. 5 ст. 33, ч. 2 ст. 228, п. "г" ч. 3 ст. 228.1, ч. 1 ст. 30, п. "г" ч. 3 ст. 228.1 , ч. 2 ст. 228 УК РФ, направлено заместителю прокурора г. Обь Новосибирской области 11 марта 2013 г.);

– описывающая действие наркотических средств;

– раскрывающая способы противодействия в процессе уголовного и административного судопроизводства;

– содержащая рекламу наркотиков и способы продажи;

– детализирующая схемы легализации денег от наркодоходов и т.д.;

3) электронные платежные системы.

Изучая данные браузера, можно установить и электронные платежные системы, которыми пользовался подозреваемый (обвиняемый).

Это могут быть платежные системы QIWI, WebMoney, Bitcoin и другие. В последнее время в преступной среде разрабатываются более сложные схемы движения денежных средств, адаптируемые под новые технологии рынка финансовых услуг. В частности, прослеживается тенденция к абсолютному исключению из процесса купли-продажи перечислений в виде реальной валюты (аккумулируемой как в наличной, так и безналичной форме).

В основном злоумышленники используют возможности электронной платежной системы QIWI. При этом кроме электронных "кошельков" выявлены случаи использования QIWI ваучеров при сбыте наркотических средств через интернет-магазины.

Использование QIWI ваучеров предполагает следующую систему взаиморасчетов: покупатель наркотических средств через свой "кошелек" в платежной системе QIWI оформляет любую сумму в виде QIWI ваучера (доступная сумма от 1 руб. до 15000 руб.), направляет оператору интернет-магазина ссылку и код ваучера для активации денежных средств, оператор активирует ваучер и может совершить любую операцию с полученными деньгами. Передача ваучера не представляет трудностей и осуществляется любым доступным способом: по мобильному телефону, с помощью программ ICQ, Skype, Jabber, по электронной почте, через социальные сети "ВКонтакте", "Facebook" и т.д.

Основным преимуществом такой системы расчетов является анонимность. Согласно данным разработчика, указанный финансовый инструмент разработан с целью повышения конфиденциальности перевода, так как все необходимые данные отправляются с почтового сервера компании, мобильный номер телефона и контактные сведения об отправителе, с "кошелька" которого сгенерирован ваучер, не указываются.

Количество операций с ваучерами для отправителей и получателей не ограничено, что позволяет беспрепятственно использовать данный способ оплаты в противоправных целях.

Новым способом оплаты за наркотики является проведение расчетов посредством криптовалюты Bitcoin. Основным преимуществом данной криптовалюты является то, что расчеты в системе Bitcoin децентрализованы. Операции между клиентами совершаются напрямую без организаций-посредников в виде банков или платежных систем, обслуживающих операции с денежными переводами, вследствие чего они носят бесконтрольный характер.

Во-вторых, для bitcoin-операций характерна полная анонимность. Несмотря на то, что все транзакции открыты для публичного просмотра, доступ к персональной информации клиентов отсутствует. Переводы в системе Bitcoin оформлены посредством цифровых подписей, которые сгенерированы в виде случайных цифро-буквенных кодов, в связи с чем идентификация отправителя и получателя практически невозможна.

Обмен валюты Bitcoin на реальные денежные средства (в том числе рубли) впоследствии осуществляется в специальных сетевых обменных пунктах, предназначенных для конвертации наиболее распространенных видов электронных денег.

При осмотре компьютера целесообразно предпринять усилия обнаружения виртуальных следов посещения сайтов по приобретению и сбыту криптовалюты Bitcoin.

6. Изучить электронную почту. Посредством нее возможно установить:

а) историю переписки, которая может содержать сведения о противоправной деятельности и преступных связях подозреваемого, а также контакты других лиц;

б) доступ к другим сетевым службам. Это позволит восстановить (неизвестные правоохранительным органам) пароли доступа к форумам, электронным платежным системам и т.д.

Работа с электронной почтой осуществляется либо через веб-страницу, либо через специальное приложение (Microsoft Outlook, TheBat!, MozillaThunderbird и т.д.).

7. Исследовать средства синхронизации данных.

Помимо локального хранения файлов пользователя все большее распространение получают средства синхронизации файлов на нескольких компьютерах и в сети (Dropbox, OneDrive, Яндекс.Диск), в которых могут быть сохранены файлы (например, фотографии), удаленные из памяти компьютера, контакты и т.п. Такие средства часто называются "облако". Эту возможность не следует недооценивать, так как синхронизация может производиться без команды пользователя, например при подключении телефона к компьютеру. Например, для осмотра облака Dropbox нужно убедиться, что соответствующая программа запущена (рядом с часами в правом нижнем углу экрана компьютера должен отображаться значок в виде открытой коробки).

Криминалистическое значение исследования средств синхронизации состоит в том, что могут быть получены данные, сохраненные с других устройств подозреваемого (смартфон, ноутбук, планшет) или удаленные им, но сохранившиеся в облаке.

8. Выявить средства анонимизации.

К ним относится программное обеспечение для сокрытия личных данных и следов пребывания пользователя при работе в сети Интернет. Использование данного программного обеспечения свидетельствует об опытности пользователя и/или его желании скрыть следы своей противоправной деятельности.

Наибольшее распространение среди средств анонимизации получила система Tor (сокр. от англ. The Onion Router – "луковый роутер"). Это система прокси-серверов, позволяющая устанавливать анонимное шифрованное сетевое соединение, защищенное от прослушивания. С пользовательской точки зрения Tor представляет собой специальный веб-браузер (на основе MozillaFirefox).

С помощью Tor пользователи могут сохранять анонимность при работе в сети Интернет при посещении сайтов, ведении блогов, отправке мгновенных и почтовых сообщений, а также при работе с другими приложениями, использующими сеть Интернет.

9. Применить средства поиска файлов.

В ходе следственного осмотра с использованием средств поиска файлов могут быть обнаружены: фотоснимки закладок, схемы проезда, специальная литература (по изготовлению наркотических средств, применению оборудования и т.д.), прейскуранты на наркотические средства, инструкции по поведению закладчика и т.д.

Это может быть сделано с помощью встроенных средств операционных систем. Поиск можно осуществлять по имени файла, дате последнего изменения и его типу. После завершения поиска по именам файлов можно выполнить поиск по содержимому файлов, для этого нужно в нижней части окна с результатами поиска нажать кнопку "Содержимое файлов".

10. Использовать программное обеспечение для восстановления недавно удаленной информации.

Значимая для расследования информация может быть удалена подозреваемым по различным мотивам (например, противодействие органам расследования). Однако в современных операционных системах удаленные файлы сначала попадают в специальный раздел (Корзина), из которого они могут быть восстановлены средствами самой операционной системы. Корзина опустошается либо по команде пользователя, либо при превышении выделенного объема (при этом самые старые файлы удаляются из корзины). Но даже при удалении без помещения файла в корзину или после очистки корзины информация сохранится до тех пор, пока на освобожденный участок носителя информации не будет записана новая информация.

Существует специальное программное обеспечение, позволяющее восстановить удаленную, но не перезаписанную инфор-

мацию, например R.saver, Recuva, RecoverMyFiles. С другой стороны, существует программное обеспечение для необратимого удаления информации (CCleaner, DataShredder). Наличие на ПК такого ПО следует рассматривать как характеризующую информацию (владелец ПК является опытным пользователем и возможно ему есть что скрывать).

При осмотре нужно минимизировать влияние на носители информации: не копировать на них новые файлы (особенно крупные), не запускать требовательные к объему памяти программы или программы для обслуживания носителей информации для исключения утраты возможности восстановления недавно удаленных файлов.

На заключительном этапе следственного осмотра при принятии решения об изъятии компьютера его целесообразно не выключать, а перевести в спящий режим (на сленге – гибернация). В этом случае сохраняется состояние всех запущенных приложений, а не только информация на жестком диске. После этого с соблюдением уголовно-процессуальных требований необходимо упаковать осмотренный объект.

Безусловно, указанный перечень действия и в более полном объеме может быть выполнен при производстве компьютерно-технической экспертизы. Однако в связи с сокращением штатной численности сотрудников правоохранительных органов, в том числе входящих в их состав экспертно-криминалистических подразделений, и существенным увеличением объектов компьютерной техники, изымаемой при производстве оперативно-розыскных мероприятий и следственных действия и направляемой на исследование, сроки производства экспертизы могут быть увеличены до 3-4 месяцев, что негативно отражается на качестве расследования уголовных дел.

Одним из вариантов выхода из сложившейся ситуации представляется применение представленного алгоритма при производстве следственных действий (отдельных видов следственного осмотра – осмотра места происшествия и осмотра предмета, а также обыска).

Библиографический список

1.Баев, О.Я. Тактика следственных действий : учебное пособие / О.Я. Баев. – М.: Юрлитинформ, 2013.

2.Клевцов, В.В. Проблемные аспекты изъятия электронных носителей информации при расследовании распространения "дизайнерских" наркотиков с использованием сети Интернет / В.В. Клевцов // Российский следователь. – 2015. – № 6.

3.Окоменко, Р.И. К вопросу о правомерности осмотра компьютера как следственного действия / Р.И. Окоменко // Законность. – 2015. – № 1.

4.Скобелкин, С.Ю. Использование специальных знаний при работе с электронными следами / С.Ю. Скобелкин // Российский следователь. – 2014. – № 20.

5.Чистова, Л.Я. Незаконные действия с сильнодействующими и ядовитыми веществами, совершенные с использованием сети Интернет / Л.Я. Чистова // Библиотека криминалиста. – 2013. – № 5.