*Вестник Томского государственного университета. 2021. № 462. С. 238–247.* DOI: 10.17223/15617793/462/29

УДК 343.98

*Н.И. Малыхина, С.В. Кузьмина*

# АЛГОРИТМ ДЕЙСТВИЙ СЛЕДОВАТЕЛЯ В ТИПОВЫХ СИТУАЦИЯХ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ

Учитывая особенности принятия тактико-управленческих решений на различных этапах деятельности следователя при расследовании мошенничеств, совершенных с использованием сети Интернет, авторами выделены типовые ситуации при проверке сообщения о преступлении, типовые ситуации первоначального и последующего этапов расследования. В каждой типовой ситуации определен алгоритм действий следователя, разработаны методические рекомендации по тактике отдельных следственных действий с учетом специфики совершаемых преступлений.

**Ключевые слова:** интернет; мошенничество; киберпреступность; типовые следственные ситуации; расследование.

В современных условиях информатизации и цифровизации всех сфер общественной и частной жизни актуальность приобретают вопросы расследования и раскрытия киберпреступлений, темпы роста которых отличаются особой динамичностью. По данным МВД РФ о состоянии преступности за 2019 г., в Российской Федерации зарегистрировано более 294 тыс. преступлений, совершенных с использованием информационных технологий, что почти на 70% превышает показатели предыдущего года [1]. В 2019 г. основной массив киберпреступлений в России (около половины от числа зарегистрированных преступлений в сфере информационных технологий) составили интернет-мошенничества, число которых в общей структуре киберпреступности увеличилось на 40% [2].

В связи с обозначенными качественными и количественными изменениями структуры преступности возрастает практическая необходимость в дополнении и совершенствовании методик расследования отдельных видов киберпреступлений, в том числе мошенничеств, совершенных с использованием сети Интернет.

Учитывая, что деятельность по расследованию и раскрытию преступлений осуществляется под воздействием факторов и процессов объективной действительности, в конкретных условиях времени, места, взаимодействия субъектов с различным процессуальным статусом, при разработке частных методик расследования преступлений целесообразным является использование ситуационного подхода.

Отдельные положения, касающиеся характеристики ситуаций, попадающих в сферу изучения криминалистики, в частности следственных, рассматривались в работах Р.С. Белкина, Л.Г. Видонова, В.К. Гавло, Л.Я. Драпкина, И.М. Лузгина, Е.Р. Россинской, Т.А. Седовой, Н.А. Селиванова, Н.П. Яблокова и других ученых. Криминалистическая ситуалогия как целостная теория ситуаций в криминалистике впервые получила освещение в работе Т.С. Волчецкой, определившей следственную ситуацию как «степень информационной осведомленности следователя о преступлении, а также состояние процесса расследования, сложившееся на любой определенный момент времени, анализ и оценка которого позволяют следователю принять наиболее целесообразные по делу решения» [3. С. 93].

Важным аспектом построения частных криминалистических методик является осуществление типизации следственных ситуаций. Однако, наряду с относительно согласованными научными воззрениями по вопросу определения основных структурных компонентов методики расследования преступлений, используемых в качестве основы при построении частных криминалистических методик, в науке отсутствует единое представление о сущности понятий «типичная» и «типовая» применительно к характеристике следственных ситуаций, что нередко приводит к отождествлению данных понятий.

В толковом словаре современного русского языка Д.Н. Ушакова термин «типовой» определяется как «являющийся образцом, типом, стандартом для ряда явлений, случаев». Термин «типичный» трактуется как «наделенный характерными особенностями, свойственными какому-либо типу, легко подводимый под тип» [4. С. 678]. Аналогичное толкование указанных терминов представлено и в иных словарях, энциклопедиях.

Проецируя данные положения на определение понятий типичных и типовых следственных ситуаций, отметим, что термин «типичный» характеризует индивидуальные ситуации, наиболее соответствующие определенному типу, а основу построения методик расследования, к примеру вида, групп преступлений, составляют типовые следственные ситуации, являющиеся более абстрактными по формулировке содержания в отличие от типичных ситуаций. Разработка именно типовых следственных ситуаций обусловлена, в частности, многообразием способов и специфики механизмов совершения преступлений, например интернет-мошенничеств, что не позволяет выделить конкретные характерологические особенности следственных ситуаций, можно лишь определить ситуации, носящие типовой характер. В этой связи уместно справедливое замечание Т.С. Волчецкой о том, что в информационной структуре типичной ситуации преобладают общие, часто повторяющиеся черты, в отличие от типовой ситуации [3. С. 105–106].

Учитывая данные положения, в целях исследования особенностей принятия тактико-управленческих решений на различных этапах деятельности следователя при расследовании мошенничеств, совершенных с использованием сети Интернет, следует выделить:

1) типовые ситуации при проверке сообщения о мошенничестве, совершенного с использованием сети

Интернет (с момента получения сообщения о преступлении до возбуждения либо отказа в возбуждении уголовного дела);

2) типовые ситуации первоначального этапа расследования мошенничеств, совершенных с использованием сети Интернет (с момента возбуждения уголовного дела до предъявления обвинения по уголовному делу);

3) типовые ситуации последующего этапа расследования мошенничеств, совершенных с использованием сети Интернет (с момента предъявления обвинения до окончания предварительного расследования).

Определение типовых следственных ситуаций и степени их распространенности на каждом из указанных этапов базируется на результатах изучения 70 приговоров по уголовным делам о мошенничествах, совершенных в сети Интернет, и проведенного опроса 82 следователей в форме онлайн-анкетирования по проблемам расследования интернет-мошенничеств. Уголовные дела за 2019 г. были рассмотрены судами на территории Саратовской, Тамбовской, Волгоградской, Пермской, Костромской, Кемеровской, Оренбургской, Ростовской, Ивановской областей, Приморского края и Республики Татарстан.

Следует отметить, что в условиях совершения интернет-мошенничеств в специфичной среде (виртуальном киберпространстве) наблюдается возможность одновременного осуществления преступной деятельности одним лицом в нескольких регионах и стирание границ интернет-преступности. Обозначенную особенность интернет-мошенничеств можно проиллюстрировать примером из следственной практики Управления уголовного розыска УМВД России по Ивановской области. При раскрытии серии мошенничеств, совершенных с использованием сети Интернет, было установлено, что криминальная деятельность преступника, проживающего в Ивановской области, насчитывала более двадцати эпизодов и распространилась на Хабаровск, Иркутск, Москву, Ярославль, Калугу, Ростов-на-Дону и другие города Российской Федерации [5].

В этой связи процессы совершения и расследования интернет-мошенничеств наименее подвержены влиянию географических и иных факторов, связанных со спецификой различных регионов, что позволяет отметить универсальность рассматриваемых типовых следственных ситуаций и алгоритма действий следователя на различных этапах при расследовании рассматриваемых преступлений.

**В ходе проведения проверки сообщения** о совершении интернет-мошенничества определены следующие типовые ситуации в зависимости от источника и объема информации.

**Ситуация 1:** *сведения о мошенничестве, совершенном с использованием сети Интернет, получены из заявления потерпевшего, иных неофициальных источников; информации для принятия итогового процессуального решения недостаточно.*

В указанной ситуации целесообразным является проведение следующих проверочных действий.

1. Получение объяснений от заявителя и лиц, указанных в первичной информации в качестве возможных свидетелей.

2. Истребование выписки о движении денежных средств с банковского счета потерпевшего.

3. Осмотр места происшествия, компьютерных и иных устройств с привлечением специалистов в области информационных технологий в целях выявления и фиксации данных, свидетельствующих о совершении преступления.

В рассматриваемой ситуации этапа проверки сообщения о преступлении осмотр проводится по месту нахождения компьютерного оборудования потерпевшего. При этом особое внимание в ходе данного осмотра следует уделить обнаружению и фиксации цифровых следов, таких как данные аккаунта пользователя в социальных сетях, переписка потерпевшего и преступника в социальных сетях и серверах для обмена сообщениями, данные журнала интернет-браузера потерпевшего, следы вывода денежных средств, log-файлы, отчеты и статистика антивирусного программного обеспечения.

В протоколе осмотра места происшествия применительно к расследованию мошенничеств, совершенных с использованием сети Интернет, указываются: 1) сведения о месте размещения компьютерных и иных устройств, их цвете, маркировочных и фирменных обозначениях, серийных номерах, внешнем состоянии и повреждениях, иных индивидуальных характеристиках (например, MAC-адрес, IP-адрес устройства), материальных следах, обнаруженных на устройствах; 2) сведения о наличии подключения компьютерных устройств к сети Интернет, виде связи сети и используемой для подключения аппаратуре (модеме); 3) состояние компьютерной техники на момент осмотра (включенное либо выключенное), описание изображения экрана, открытых файлов, выполняющихся программ и запущенных процессов при включенном состоянии оборудования [6. С. 129]; 4) порядок проводимых действий с оборудованием, последовательность открывания веб-страниц, окон и файлов, в которых содержались цифровые следы мошенничества (например, применительно к осмотру страницы потерпевшего в социальной сети в первую очередь указывается способ доступа к странице, персональный идентификатор страницы, сведения о содержании главной страницы пользователя, его анкетных данных, затем осуществляется последовательный переход к страницам «Настройки», «Безопасность» для установления сведений об истории активности, к странице «Сообщения», страницам других пользователей с фиксацией в протоколе криминалистически значимой информации); 5) применимые дополнительные способы фиксации цифровых следов (скриншоты экрана и др.); 6) наименование файлов, подлежащих копированию в ходе осмотра (log-файлов, сохраненных веб-страниц, электронных документов), способ копирования с указанием используемого программного обеспечения и технических средств, носителей информации, количества изготовленных копий; 7) порядок выключения и изъятия компьютерных и сетевых устройств (компьютерные устройства изымаются в выключенном состоянии либо в состоянии «спящего режима» для сохранения данных оперативной памяти в случае изъятия порта-

тивных компьютеров; вопросы, связанные с процессом выключения компьютерных устройств, рекомендуется согласовывать со специалистом для предотвращения утраты значимых следов).

**Ситуация 2:** с*ведения о мошенничестве, совершенном с использованием сети Интернет, получены по результатам оперативно-розыскной деятельности; информации для принятия итогового процессуального решения достаточно.*

В указанной ситуации результаты оперативно-розыскной деятельности, предоставленные для решения вопроса о возбуждении уголовного дела, подлежат рассмотрению с точки зрения достаточности данных, указывающих на признаки преступления; наличия сведений о месте, времени, обстоятельствах преступления, признаки которого обнаружены; о лицах, совершивших интернет-мошенничество (если они известны); о местоположении предметов, которые могут стать вещественными доказательствами.

На практике наиболее часто на этапе проверки сообщения о преступлении возникают ситуации первого типа, характеризующиеся недостаточностью первичной информации о наличии признаков преступления (95%), значительно реже встречаются ситуации второго типа (5%), что подтверждается результатами проведенного в ходе настоящего исследования анкетирования следователей.

Итоговым процессуальным решением на рассматриваемой стадии выступает постановление об отказе в возбуждении уголовного дела либо постановление о возбуждении уголовного дела, являющееся основанием для начала предварительного расследования.

**На первоначальном этапе расследования** мошенничеств, совершенных с использованием сети Интернет, определены в зависимости от содержания исходной информации следующие типовые ситуации.

**Ситуация 1:** у*становлены способ совершения интернет-мошенничества, потерпевшие и свидетели, выявлены отдельные цифровые следы, данные о лице, совершившем преступление, отсутствуют.*

В данной ситуации выявленные отдельные цифровые следы (например, следы неправомерного доступа к аккаунту в социальных сетях, доменное имя сайта мошеннического интернет-магазина и следы оформления заказа на сайте, следы соединений между абонентскими устройствами, следы вывода денежных средств с банковских счетов) могут служить источником информации о лице, совершившем преступление.

Направление расследования в данной ситуации сводится к установлению информации о лице, совершившем интернет-мошенничество, по оставленным следам.

Для обозначенной следственной ситуации характерен следующий алгоритм действий следователя.

1. Допросы потерпевших, в ходе которых в зависимости от примененного способа интернет-мошенничества и вида выявленных цифровых следов выяснению подлежат следующие вопросы: имеется ли у потерпевшего по месту проживания или работы персональный компьютер, мобильный телефон, планшет с доступом к сети Интернет; имеет ли кто-либо помимо потерпевшего доступ к компьютеру, мобильному телефону, планшету; зарегистрирован ли потерпевший в социальных сетях и под какой учетной записью; известны ли кому-либо, помимо потерпевшего, входные данные (логин, пароль) для доступа к профилю в социальной сети; имеются ли у потерпевшего банковские счета, карты и в каких банках, подключены ли у потерпевшего услуги «Онлайн-банк», «Мобильный банк», известны ли реквизиты карты / счета потерпевшего третьим лицам; производились ли потерпевшим платежи в пользу каких-либо сайтов, интернет-магазинов, физических лиц и в каких целях, с каких банковских счетов и на какие; с помощью каких технических средств осуществлялась плата; каким образом осуществлялась связь потерпевшего и мошенника (номера мобильных телефонов, переписка с использованием СМС, электронной почты, мессенджеров); обладал ли мошенник какими-либо особенностями голоса, речи; сталкивался ли потерпевший с фактами несанкционированного удаленного доступа к персональному компьютеру; имеются ли на компьютерном устройстве потерпевшего программы, препятствующие несанкционированному удаленному доступу; устанавливались ли на компьютерные устройства потерпевшего программы, после которых на устройствах проявлялась подозрительная активность (самостоятельное подключение к сети, появление нехарактерных ошибок, автоматический запуск программ и файлов, выключение устройства).

2. Изучение выписок о движении денежных средств на банковских счетах потерпевшего.

3. Направление запросов в банки и кредитные организации о предоставлении данных владельца счета, на который в результате мошенничества были перечислены денежные средства.

4. Направление запросов регистраторам доменного имени о предоставлении сведений об администраторе (владельце) доменного имени сайта мошеннического интернет-магазина.

5. Направление запроса информации оператору связи о лице, на которое зарегистрирован абонентский номер.

6. Направление запросов провайдерам о предоставлении информации об интернет-соединениях абонента или абонентского устройства (указанная информация, предоставленная провайдером, может содержать сведения о дате и времени добавления записи по системному времени сервера соединений; IP-адрес маршрутизатора, обслуживающего данную сессию, login пользователя, наименование линии, вид соединения, тип записи (start, stop, update) и дополнительные параметры); сведения об интернет-соединениях имеют важное значение для расследования интернет-мошенничества и позволяют установить, кто использовал известный IP-адрес в заданный промежуток времени (по записям типа stop).

В рассматриваемой следственной ситуации практические работники сталкиваются с трудностями, вызванными отсутствием необходимого и оперативного содействия банков, интернет-провайдеров, регистраторов доменных имен при предоставлении ответов на запросы. Это отмечают 60% опрошенных следователей.

7. Допросы свидетелей, к которым в силу специфики преступления могут относиться лица, обладающие криминалистически значимой информацией ввиду профессионального статуса (представители регистратора доменных имен, провайдера хостинга, сотрудники банков и кредитных организаций).

При допросе представителя регистратора доменных имен выяснению подлежат сведения о порядке регистрации доменных имен, лице, осуществившем приобретение конкретного домена, выполненных платежах для регистрации доменного имени и наличии подтверждающих документов об этом.

Представитель компании провайдера может быть допрошен в качестве свидетеля относительно сведений о логинах, анкетных данных, адресах абонентских подключений, конкретных внешних IP-адресах, с которых осуществлялся доступ к сети Интернет, типе IP-адреса (статический либо динамический), сроках и порядке заключения договора на предоставление интернет-соединений.

Работники банковских и кредитных организаций подлежат допросу по вопросам осуществления банковского обслуживания счетов, принадлежащих потерпевшему либо преступнику, и проведения ими банковских операций, установления размера несанкционированно переведенных денежных средств и номеров банковских счетов; определения статуса операций по переводу денежных средств (была ли проведена операция или попытка перевода денежных средств, которая не удалась по техническим причинам, что будет свидетельствовать о покушении на хищение денежных средств).

Следует отметить, что допрос представителей регистраторов доменных имен, компаний-провайдеров, сотрудников банков может осуществляться по иным вопросам, конкретизирующим и разъясняющим информацию, представленную в ответе на запрос следователя в рамках расследования уголовного дела.

8. Назначение и проведение необходимых экспертиз.

9. Направление поручения органам дознания о проведении оперативно-розыскных мероприятий, направленных на установление лиц, причастных к совершению мошенничества в сети Интернет.

10. При наличии возможности принятие необходимых мер для задержания подозреваемых с последующим проведением допросов задержанных лиц.

**Ситуация 2:** у*становлены способ совершения интернет-мошенничества, потерпевшие и свидетели, цифровые следы не выявлены, данные о лице, совершившем преступление, отсутствуют.*

Данная следственная ситуация, обусловленная легкостью уничтожения и модификации цифровых следов, может возникать в связи с неосторожными либо умышленными действиями потерпевших (например, удаление истории веб-браузера, журнала вызовов, сообщений в социальных сетях) и преступника (например, использование программного обеспечения для сокрытия присутствия в системе вредоносных программ; удаление сайта интернет-магазина или аккаунта в социальной сети, с использованием которых осуществлялось мошенничество), а также в связи с техническими особенностями работы компьютерных и мобильных устройств (например, автоматическое уничтожение следов, хранящихся в оперативной памяти, при отключении компьютерного устройства; уничтожение следов при повреждении компьютерных и мобильных устройств).

Разрешение данной следственной ситуации осуществляется путем выявления следов совершения преступления (преимущественно цифровых) с применением специальных знаний и технических средств для последующего установления лица, совершившего мошенничество с использованием сети Интернет.

Для реализации указанного направления расследования проводятся действия по следующему алгоритму.

1. Допросы потерпевших с целью получения сведений о предпринятых ими возможных действиях, повлекших уничтожение цифровых следов, а также запомнившейся им информации, содержащейся в цифровых следах (например, сохранившиеся в памяти допрашиваемого сведения о доменном имени, конфигурации, внешнем виде сайта мошеннического интернет-магазина, сведения об анкетных, контактных и иных данных, указанных мошенником в социальной сети, сведения об абонентском номере мошенника, дате и времени соединения, данные о содержании переписки с преступником в мессенджерах и социальных сетях).

Например, в Тюменской области в ходе расследования уголовного дела по факту мошенничества с использованием интернет-магазина, сайт которого впоследствии был заблокирован и недоступен для просмотра, при допросе потерпевших следователям удалось получить информацию о наименовании интернет-магазина, адресе, контактных данных, указанных на данном сайте, что способствовало установлению подозреваемых [7].

2. Направление запроса регистратору доменного имени с целью получения сведений об администраторе (владельце) доменного имени и основаниях аннулирования домена сайта мошеннического интернет-магазина (в случае, если в ходе допроса потерпевших получена информация о доменном имени сайта).

3. Направление запроса оператору связи о соединениях по абонентскому номеру потерпевших за определенный период (в случае, если в ходе допроса потерпевших получена ориентировочная информация о дате и времени соединения с мошенником по телефону).

4. Допросы свидетелей, в том числе представителей регистратора доменных имен и оператора связи, по вопросам, связанным с установлением информации, содержащейся в цифровых следах, а также по иным вопросам (например, связанным с разъяснением ответов на запросы следователя).

5. Выемка и осмотр компьютерных и мобильных устройств потерпевших с участием специалистов и применением специальных технических средств.

Важным аспектом при проведении обозначенных следственных действий в данной ситуации являются подбор и эффективное использование программных и технических средств, позволяющих осуществлять обнаружение и изъятие уничтоженных цифровых следов. Например, для извлечения и копирования

файлов операционных систем компьютерных и мобильных устройств могут использоваться переносная лаборатория «RM3», аппаратно-программные комплексы «UFED», позволяющие извлекать удаленные файлы и пароли; для поиска, сбора и восстановления следов использования интернет-браузеров может быть использована программа «NetAnalysis».

Кроме того, при осмотре компьютерных устройств целесообразно использование комплектов аппаратных блокираторов записи («ForensicPC Ultimate Write Block Kit», «DriveLock Firewire/USB»), позволяющих просматривать файлы, хранящиеся на устройстве, без опасности внесения в них каких-либо изменений.

6. Назначение судебной компьютерной и иных экспертиз.

В ходе судебной компьютерной экспертизы по делам о расследовании мошенничеств, совершенных с использованием сети Интернет, могут быть разрешены следующие вопросы: каковы марка, модель, технические характеристики, MAC-адрес представленного на исследование объекта; какая информация, содержащая конкретный перечень данных или ключевые слова имеется в памяти компьютерного устройства; совершалось ли с помощью представленных компьютерных устройств подключение к сети Интернет, для доступа к каким ресурсам сети Интернет и в какие промежутки времени; осуществлялась ли посредством использования представленного на исследование оборудования электронная почтовая переписка, каковы реквизиты адресата и отправителя, время направления / получения сообщений; имеются ли на представленном компьютерном или мобильном устройстве сведения, подтверждающие использование кредитных карт для проведения электронных платежей и др. Формулировки вопросов при назначении компьютерной экспертизы целесообразно предварительно согласовать с экспертом или специалистом.

В случае обнаружения в ходе осмотра переписки потерпевшего и лица, совершившего преступление (в социальных сетях и серверах для обмена сообщениями), может проводиться судебная автороведческая экспертиза текстов электронных сообщений. В некоторых случаях при расследовании интернет-мошенничеств возможно проведение психологической, комплексной психолого-психиатрической, психолингвистической экспертиз.

Также при разрешении данной следственной ситуации необходимо проведение ранее обозначенных действий, направленных на установление личностных особенностей преступника.

**Ситуация 3:** *установлены способ совершения интернет-мошенничества, потерпевшие и свидетели, выявлены цифровые следы, известны некоторые данные о лице, совершившем преступление, но его местонахождение неизвестно.*

На первоначальном этапе расследования в обозначенной ситуации могут быть известны фамилия, имя, отчество лица, совершившего преступление, установленные, например, на основании данных профиля мошенника в социальной сети или по номеру его банковской карты / счета, на которые были перечислены денежные средства через сервисы онлайн-банков.

В рассматриваемой ситуации расследование преступления осуществляется путем проверки достоверности имеющихся сведений о лице, совершившем преступление, и установления его местонахождения. При этом предопределяются следующие следственные и иные действия.

1. Допросы потерпевших и свидетелей с целью детализации сведений о преступнике и возможном месте его нахождения.

2. В случае наличия информации о номере мобильного телефона, принадлежащего мошеннику, целесообразно направление запроса информации оператору связи о лице, на которое зарегистрирован абонентский номер, и о соединениях по абонентскому номеру, а также направление поручения органам дознания о проведении необходимых оперативно-розыскных мероприятий (снятие информации с технических каналов связи и др.).

3. Проверка и истребование информации о преступнике и его месте жительства по базам ИЦ и ГИАЦ, при наличии судимости у проверяемого лица целесообразно истребование дактилоскопической карты, фотографий, характеризующего материала из места отбытия наказания. Истребование информации о преступнике по указанным базам целесообразно и в силу того, что в некоторых случаях интернет-мошенничества совершаются гражданами, содержащимися под стражей в исправительных учреждениях. Например, в Ивановской области, по статистике за 2018–2019 гг., подобные мошеннические действия составили подавляющее большинство в числе хищений, совершенных с использованием информационных технологий [8].

4. Направление поручения органам дознания о проведении мероприятий по розыску мошенника.

5. Задержание и допрос подозреваемых.

6. Проведение осмотра мест применения компьютерного оборудования и осмотра компьютерных устройств, использованных для совершения преступления.

Обнаружению и внешнему осмотру подлежат компьютерные, мобильные устройства; устройства соединения с интернет-сетью; специальная литература, посвященная интернет-технологиям; платежные документы; распечатанные на бумажных носителях реквизиты банковских карт; адреса электронной почты, пароли; «скрипты» диалогов с клиентами мошеннических интернет-магазинов; документы на предоставление интернет-услуг, услуг сотовой связи. Компьютерные устройства, а также клавиатуру, компьютерную мышь, сканеры, принтеры, роутер, модемы необходимо осмотреть на предмет наличия следов рук, кожных покровов человека, следов биологического происхождения.

В рамках этого следственного действия изучается внешний вид устройства (его марка, модель, цвет, конструкция, фоновый рисунок, повреждения, потертости) и проходит осмотр аппаратного обеспечения (жесткого диска, оперативной памяти и сетевой карты компьютера, на которой указывается MAC-адрес устройства; аккумуляторной батареи, микропроцессора, дисплея, клавиатуры, фото- и видеокамеры, интерфейсов связи мобильного телефона).

Значимым действием осмотра выступает определение типа операционной системы, IMEI (для мобильного телефона), IP-адреса и MAC-адреса устройства. Применительно к осмотру мобильного устройства код IMEI, операционная система, версия прошивки, IP-адрес, MAC-адрес, модель и серийный номер телефона указываются в разделе «Настройки» – «Об устройстве». Код IMEI, являющийся уникальным идентификатором мобильного устройства, также указывается под аккумуляторной батареей либо на задней поверхности крышки мобильного телефона и может быть отображен на экране аппарата в результате набора на клавиатуре комбинации знаков – «*#06#».

При осмотре компьютерного устройства тип операционной системы может быть определен по характерному виду графического интерфейса и логотипам (Microsoft Winodws: XP, Vista, 7, 8, 10; Mac OS) либо посредством изучения сведений о системе, которые отражаются, например, в разделах «Панель управления» – «Система и безопасность» – «Система» (для Microsoft Winodws 10). IP-адрес и MAC-адрес компьютерного устройства отображаются при переходе по значку сетевого соединения в правом нижнем углу экрана монитора, в разделах «Параметры сети и Интернет» – «Wi-Fi» либо «Ethernet» – «Свойства оборудования» (для Microsoft Winodws 10). Следует отметить, что наименования указанных разделов, содержащих сведения о свойствах оборудования, могут отличаться в зависимости от типа операционной системы. IP-адрес, указанный в свойствах компьютера, начинающийся на 10, 100.64, 172.16 или 192.168, является внутренним (имеет значение только в локальной сети). В целях установления внешнего IP-адреса устройства необходимо с помощью любого браузера перейти на специализированный сайт (например, «myip.ru» или «2ip.ru»).

Осмотр мобильных устройств сопровождается изучением списка контактов, журнала вызовов, СМС-сообщений. При большом объеме контактов и СМС-сообщений целесообразно использовать выборочный способ осмотра, заключающийся в использовании функции поиска или фильтра.

Кроме того, при осмотре мобильных и компьютерных устройств целесообразно изучить данные интернет-браузеров, истории просмотра веб-страниц и закладок, в частности, социальных сетей, страниц электронных платежных систем, электронной почты в целях выявления следов преступления.

В рамках осмотра веб-страниц в сети Интернет следователю при участии специалиста целесообразно установить и отразить в протоколе доменное имя сайта и администратора домена (владельца сайта); проверить соответствие символьного адреса сайта его настоящему IP-адресу посредством трассировки, чтобы убедиться в том, что браузер отображает страницы подлинного сайта; зафиксировать содержание сайта в сети Интернет посредством описания внешнего вида, структуры сайта, расположения гиперссылок, текстового содержания и количества страниц сайта. Детальному описанию подвергаются страницы, содержащие криминалистически значимую информацию о совершенном преступлении.

Все проводимые в ходе осмотра веб-страниц процедуры и переходы по ссылкам необходимо фиксировать в протоколе осмотра с указанием даты и времени, URL страниц, IP-адресов, технических средств, с помощью которых проводился осмотр. Ход и результаты осмотра интернет-страниц дополнительно фиксируются с помощью скриншотов экрана сайта (при нажатии на клавиатуре клавиши «Print Screen»), что является специфическим способом фиксации цифровых следов.

При осмотре электронной почты следует обратить внимание на вложения, содержащиеся в сообщении, к которым могут относиться текстовые документы, изображения, видеофайлы. Наличие и содержание указанных вложений также целесообразно отразить в протоколе следственного действия. В протоколе осмотра электронной почты указываются сведения о служебном заголовке сообщения (имена и электронные адреса отправителя и получателя сообщения, тема, дата, время отправки, получения сообщения), первые слова текста, последние фразы, содержание вложений. Сообщения, содержащие криминалистически значимую для расследования информацию, целесообразно отражать в протоколе дословно.

Таким образом, разрешение типовых следственных ситуаций первоначального этапа расследования мошенничеств, совершенных с использованием сети Интернет, сводится к собиранию и исследованию максимального объема доказательств и установлению лиц, причастных к совершению преступления.

**Последующий этап расследования**, в отличие от первоначального, как правило, характеризуется наличием необходимого объема собранной по делу доказательственной информации и в большей степени направлен на закрепление и проверку имеющихся в уголовном деле доказательств.

На последующем этапе расследования мошенничеств, совершенных с использованием сети Интернет, определены типовые ситуации в зависимости от степени признания вины обвиняемого и достаточности доказательств.

**Ситуация 1:** *обвиняемый признает свою вину в совершении преступления, дает показания относительно обстоятельств преступления и соучастников, что подтверждается доказательствами по уголовному делу.*

Указанная типовая ситуация последующего этапа расследования является для следователя наиболее благоприятной. Действия следователя в данной ситуации направлены на систематизацию полученных по делу доказательств и совершение процессуальных действий, необходимых для окончания предварительного расследования.

При этом целесообразно проведение следующих следственных действий.

1. Допрос обвиняемого с целью детализации сведений об обстоятельствах и эпизодах криминальной деятельности (о способах подготовки, совершения, сокрытия интернет-мошенничества, соучастниках и роли каждого из них в совершении преступления).

Допрос обвиняемого по делам о мошенничествах, совершенных с использованием сети Интернет, требует особой подготовки. На подготовительном этапе допроса целесообразно детально изучить материалы уголовного дела и личностные особенности допрашиваемого. При этом источником информации о личностных качествах допрашиваемого и некоторых фактах его биографии могут быть социальные сети [9. С. 8]. Например, анализ списка друзей и групп пользователя в социальной сети позволяет установить круг общения и личных интересов, публикуемые записи и комментарии пользователя на странице опосредованно могут свидетельствовать об отношении лица к определенным социальным явлениям и событиям [10. С. 164].

При подготовке к допросу следователю целесообразно изучить специальную литературу, посвященную информационным технологиям, используемым в ходе совершения преступления; провести консультации со специалистами в области IT-технологий для правильной постановки вопросов, учитывая специфику способа преступления.

В ходе допроса выяснению подлежат общие вопросы о наличии у обвиняемого персонального компьютера с доступом к сети Интернет, навыков работы с компьютерной техникой и интересующим программным обеспечением; должности и месте работы; времени возникновения умысла на совершение мошенничества с использованием интернет-технологий, мотивах, целях. Далее в ходе допроса необходимо детализировать данные о способе конкретного преступления, о следах, которые могли остаться в результате совершения преступления.

Например, в ходе допроса обвиняемого в мошенничестве, совершенном с использованием интернет-магазина, выяснению подлежат вопросы, связанные с установлением времени создания и действия сайта интернет-магазина; технических средств, программного обеспечения, конструкторов, использованных для создания сайта; зарегистрированного доменного имени сайта; товаров, подлежащих продаже на сайте, способов и ресурсов рекламирования интернет-магазина и привлечения потенциальных клиентов; способов связи с потенциальными клиентами, используемых номеров телефонов с указанием их владельцев, адресов электронной почты; способов оплаты товара и реквизитов банковских счетов мошенника, на которые поступала оплата; способов сокрытия преступления.

При допросе обвиняемого в мошенничестве, совершенном с использованием социальных сетей, выяснению подлежат способы преодоления защиты информации: использованные средства подбора логинов и паролей для доступа к сети либо похищения паролей посредством перехвата информации.

Допрос обвиняемого, совершившего мошенничество с использованием вредоносных программ, характеризуется выяснением сведений об использованном языке программирования при создании вредоносной программы (С++, Си, Java, C#,), кодах вредоносных программ и их функциональном назначении, средствах управления версиями программного кода, средствах управления базами данных, способах распространения вредоносного программного обеспечения.

2. Очная ставка при наличии противоречий в имеющихся по делу показаниях.

3. Обыск (либо выемка) в случае указания обвиняемым в ходе допроса ранее неизвестных следствию мест нахождения предметов, документов, имеющих значение для уголовного дела.

При подготовке к обыску или выемке в ходе расследования мошенничества, совершенного с использованием сети Интернет, целесообразно выяснить, какие средства вычислительной техники находятся в месте производства следственного действия, оснащены ли они программами защиты информации от несанкционированного доступа (по возможности установить коды доступа к компьютерной технике), определить расположение и тип источников электропитания, пункты отключения электропитания в месте производства следственного действия, подготовить необходимые технические средства для производства обыска или выемки, пригласить для участия в производстве следственного действия специалистов и понятых. В силу того, что следователю необходимо сконцентрировать внимание на поведении обыскиваемого лица при проведении обыска, рекомендуется получить и изучить данные о личностных особенностях обыскиваемого лица, что позволит оптимизировать процесс наблюдения за его поведением [11. С. 82].

В научной литературе встречаются рекомендации о необходимости привлечения в качестве понятых лиц, обладающих специальными знаниями в сфере компьютерной информации. Указанная рекомендация небезосновательна, поскольку понятому как лицу, удостоверяющему факт производства и ход следственного действия, следует понимать смысл и содержание происходящих событий. Однако полагаем, что реализация данной рекомендации в практической деятельности, в том числе в большинстве случаев в условиях необходимости незамедлительного производства следственного действия, является трудновыполнимой.

В ходе обыска при расследовании мошенничества, совершенного с использованием сети Интернет, целесообразно максимально ограничить лицо, в помещении которого проводится обыск, в доступе к электронным устройствам и исключить его свободное передвижение.

По результатам обыска или выемки составляется протокол, изымаются необходимые предметы. В протоколе фиксируются место и обстоятельства, при которых обнаружены компьютерное оборудование, иные предметы, документы, факт добровольной выдачи или принудительного изъятия предметов; указывается перечень изымаемых предметов с описанием моделей и номерных знаков, частных признаков; фиксируется наименование, объем обнаруженных файлов, подлежащих копированию с указанием данных и характеристик накопителя; обозначается факт копирования и передачи информации законному владельцу при наличии соответствующего ходатайства, являющегося прило-

жением к протоколу, либо фиксируется отказ в удовлетворении указанного ходатайства.

4. Проверка показаний на месте в целях детализации сведений о механизме совершения мошенничества, совершенного с использованием сети Интернет.

**Ситуация 2:** *обвиняемый признает свою вину в совершении преступления, но в материалах уголовного дела содержится недостаточное количество доказательств его виновности.*

Направлением расследования в обозначенной ситуации является получение новых доказательств по делу, предопределяя следующие действия.

1. Проведение повторных допросов обвиняемого, свидетелей, потерпевших с целью установления дополнительных источников доказательств.

2. Использование в ходе расследования специальных знаний в виде проведения исследований и экспертиз.

В качестве примера эффективного использования специальных знаний в рассматриваемой следственной ситуации можно привести уголовное дело по факту мошенничества с использованием интернет-магазина в Тюменской области. В рассматриваемом деле обвиняемый в ходе дачи показаний подтвердил, что он принимал решения в компании, осуществляющей деятельность с использованием мошеннического интернет-магазина, был ее фактическим руководителем, давал указания менеджерам, составлял «скрипты» диалогов с клиентами, при этом юридически директором компании являлось иное лицо. Данные показания были подтверждены в ходе допросов работников компании, а также в ходе проведения судебной почерковедческой экспертизы, согласно выводам которой рукописные записи, подписи в договорах компании, в том числе договоре об оказании услуг по созданию сайта мошеннического интернет-магазина, выполнены обвиняемым, а не номинальным директором компании [7].

3. Поручения, адресованные органам дознания, о проведении оперативно-розыскных мероприятий, направленных на получение новых данных, относящихся к предмету доказывания.

**Ситуация 3:** *обвиняемый отрицает свою вину в совершении преступления полностью или частично, но в материалах дела содержится достаточное количество доказательств, подтверждающих вину.*

В данной ситуации возможно проявление активного противодействия расследованию со стороны обвиняемого в форме дачи ложных показаний либо отказа от дачи показаний. Основное направление расследования в этой ситуации заключается в систематизации имеющихся источников доказательственной информации и поиске новых, проверке (опровержении или подтверждении) данных обвиняемым показаний.

В указанной следственной ситуации необходимо провести следующие действия.

1. Повторный допрос обвиняемого с изменением тактики допроса.

При этом наибольшей эффективностью при расследовании преступлений в сфере информационных технологий обладают следующие тактические приемы: маскировка главного вопроса второстепенными; разъяснение допрашиваемому возможности установления того или иного факта путем проведения экспертизы, создание впечатления о бóльшей осведомленности следователя об обстоятельствах совершения преступления [12. С. 124].

Тактические приемы допроса в указанной следственной ситуации следует использовать с учетом личностных особенностей допрашиваемого. Например, при допросе интернет-мошенников, не ведущих активную социальную жизнь вне виртуального пространства, в том числе не обладающих устойчивыми криминальными связями, эффективным приемом воздействия может выступить разъяснение тяжести и последствий ответственности за совершенное преступление. В ходе допроса лиц, обладающих высоким уровнем знаний в сфере информационных технологий (например, лиц, совершивших мошенничество, сопровождающееся использованием компьютерных вирусов и программ), целесообразным является акцентирование внимания на положительных качествах и профессиональных навыках допрашиваемого.

2. Уточнение роли обвиняемого в подготовке, совершении, сокрытии преступления; установление иных лиц, причастных к преступному событию.

Обобщая вышеизложенное, укажем основные выводы по исследуемой тематике.

1. В криминалистической литературе недостаточно разработаны вопросы разграничения типичных и типовых следственных ситуаций, что нередко приводит к отождествлению данных понятий при формировании положений частных методик расследования преступлений. Анализ смысловых значений терминов «типичный» и «типовой» сквозь призму определения ситуаций расследования интернет-мошенничеств позволил установить, что при разработке частных криминалистических методик целесообразнее использовать термин «типовые» применительно к следственным ситуациям.

На основе изучения материалов судебной практики по уголовным делам об интернет-мошенничествах, проведенного опроса следователей по проблемам расследования данных преступлений выделены типовые ситуации этапов работы – при проверке сообщения о преступлении, типовые ситуации первоначального и последующего этапов расследования.

2. Установлено, что этапу проверки сообщения о совершении интернет-мошенничества, в зависимости от источника и объема информации, присущи две ситуации: а) недостаточно первичной информации о наличии признаков преступления, что обусловливает необходимость проведения проверочных действий (истребование выписок о движении денежных средств с банковского счета потерпевшего, осмотр места происшествия и компьютерных устройств с применением специальных технических средств и программ и др.) (95%); б) информации для принятия итогового процессуального решения достаточно; имеющиеся материалы подлежат рассмотрению с точки зрения достаточности данных, указывающих на признаки преступления; сведений о месте, времени, обстоятельствах преступления, признаки которого обнаружены;

о местоположении предметов, которые могут стать вещественными доказательствами, и др. (5%) (по результатам анкетирования следователей).

3. Первоначальный этап расследования мошенничеств, совершенных с использованием сети Интернет, в большинстве случаев характеризуется отсутствием сведений о мошеннике, при наличии данных о способе совершения преступления, установлении потерпевших и свидетелей, выявлении цифровых следов. Расследование осуществляется путем установления информации о лице, совершившем интернет-мошенничество, по оставленным следам (80%).

Также для данного этапа расследования характерна ситуация, определяющаяся идентичными обстоятельствами, но отсутствием цифровых следов (17,5%). Разрешение этой следственной ситуации осуществляется путем выявления цифровых следов преступления с применением специальных знаний и технических средств для последующего установления лица, совершившего мошенничество с использованием сети Интернет. Значительно реже имеет место ситуация, характеризующаяся установлением цифровых следов, способа совершения преступления, потерпевших и свидетелей, наличием отдельных сведений о преступнике, но отсутствием данных о его местонахождении. Расследование преступления направлено на проверку достоверности имеющихся сведений о лице, совершившем преступление, и установление его местонахождения (2,5%) (по результатам анкетирования следователей).

4. Три типовые ситуации последующего этапа расследования данных преступлений выделены в зависимости от степени признания вины обвиняемого и достаточности доказательств. Наиболее распространенной определена ситуация, характеризующаяся признанием обвиняемым своей вины и наличием необходимых доказательств по делу. Действия следователя в данной ситуации направлены на систематизацию полученных по делу доказательств и совершение процессуальных действий, необходимых для окончания предварительного расследования (90%). Также выявлены ситуации, когда: 1) обвиняемый признает свою вину в совершении преступления, но в материалах уголовного дела содержится недостаточное количество доказательств его виновности (расследование направлено на получение новых доказательств по делу) (4%); 2) обвиняемый отрицает свою вину в совершении преступления полностью или частично, но в материалах дела содержится достаточное количество доказательств, подтверждающих вину (расследование направлено на систематизацию имеющихся и поиск новых источников доказательственной информации, проверку – опровержения или подтверждения данных обвиняемым показаний) (6%) (по результатам изучения материалов судебной практики).

5. Разработка типовых следственных ситуаций и рекомендаций по их разрешению имеет существенное значение для совершенствования теоретико-прикладных положений методики расследования мошенничеств, совершенных с использованием сети Интернет. Практическая значимость данных положений определяется их общей направленностью на совершенствование и повышение эффективности деятельности по расследованию указанных преступлений.

## ЛИТЕРАТУРА


1. Краткая характеристика состояния преступности в Российской Федерации за январь-декабрь 2019 // Официальный сайт МВД РФ. URL: https://xn--b1aew.xn--p1ai/reports/item/19412450/ (дата обращения: 29.02.2020).
2. В МВД оценили ущерб от киберпреступлений в России в 2019 году // Сетевое издание «Russia Today». URL: https://russian.rt.com/russia/news/696185-mvd-kiberprestuplenie-statistika (дата обращения: 29.02.2020).
3. Волчецкая Т.С. Криминалистическая ситуалогия / под ред. проф. Н.П. Яблокова. М. : Калининград, 1997. 248 с.
4. Ушаков Д.Н. Толковый словарь современного русского языка. М. : Аделант, 2014. 800 с.
5. В Ивановской области полицейские раскрыли серию мошенничеств через Интернет // Официальный сайт МВД РФ. URL: https://xn--b1aew.xn--p1ai/news/item/8984038 (дата обращения: 12.07.2019).
6. Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет : дис. …канд. юрид. наук. М., 2018. 197 с.
7. Приговор Ленинского районного суда г. Тюмени № 1-20/2019 1-718/2018 от 16 мая 2019 г. по делу № 1-20/2019 // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/HxP89erYhSxq/?regular-txt=&regular-case_doc=1-20%2F2019&regular-lawchunkinfo=&regular-date_from=01.05.2019&regular-date_to=12.07.2020&regular-workflow_stage=&regular-area=&regular-court=&regular-judge=Бухарова+Амина+Салимьяновна+%28Ленинский+районный+суд+г.Тюмени+%28Тюменская+область%29%29&_=1594544617793 (дата обращения: 12.07.2019).
8. Отчет врио начальника УМВД России по Ивановской области полковника полиции В.А. Пронина перед депутатами Ивановской областной Думы от 28 марта 2019 г. // Официальный сайт УМВД РФ по Ивановской области. URL: https://37.мвд.рф/отчет-начальника-умвд-россии-по-ивановск (дата обращения: 12.07.2019).
9. Алексеева Т.А., Ахмедшин Р.Л., Юань В.Л. Исследование личности обвиняемого посредством анализа материала социальных сетей // Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы и перспективы противодействия преступлениям, совершаемым с применением информационных технологий : сб. науч. ст. / отв. ред. С.И. Давыдов, В.В. Поляков. Барнаул : Изд-во Алт. ун-та, 2018. Вып. XV. С. 7–14.
10. Шевченко Е.С. Социально-технологические детерминанты следственных действий при расследовании киберпреступлений // Актуальные проблемы российского права. 2016. № 10 (71). С. 160–169.
11. Ахмедшин Р.Л. Некоторые психологические аспекты проведения обыска // Вестник Томского государственного университета. 2011. № 348. С. 82–85.
12. Поляков В.В., Ширяев А.В. Проблемы тактики допроса по делам о компьютерных преступлениях // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2015. № 15-1. С. 123–126.



Статья представлена научной редакцией «Право» 24 сентября 2020 г.


**The Algorithm of the Investigator's Actions in Typical Situations of Internet Fraud Investigations**


*Vestnik Tomskogo gosudarstvennogo universiteta – Tomsk State University Journal,* 2021, 462, 238–247.
DOI: 10.17223/15617793/462/29

**Natalya I. Malykhina,** Saratov State Academy of Law (Saratov, Russian Federation). E-mail: nim1707@yandex.ru
**Svetlana V. Kuzmina,** Consulting Plus, LLC (Saratov, Russian Federation). E-mail: kuz44ina.svet@yandex.ru
**Keywords:** Internet; fraud; cybercrime; typical investigative situations; investigation.

The article considers the creation of theoretical and applied provisions for supplementing and improving the methodology of Internet fraud investigations. The aim of the study was to identify typical situations of investigation of these crimes and to develop the algorithm of the investigator's actions in these situations. The methodological basis of the research was the dialectical method, modeling, the system-structural method, the specific sociological method, the method of expert assessments, logical methods. The situational approach was used. Considering the peculiarities of making tactical and managerial decisions at various stages of the investigator's activity in Internet fraud investigations, the typical situations of checking crime reports and of the initial and subsequent stages of the investigation have been identified. The determination of typical investigative situations at each of the indicated stages was based on the results of the study of materials of judicial practice in criminal cases on Internet frauds, a survey of investigators on the problems of investigating these crimes. It has been revealed that the stage of checking the report of Internet fraud, depending on the source and amount of information, is characterized by two situations: either by the lack of primary information about the presence of signs of a crime (95%), or, conversely, by information sufficient to make a final procedural decision (5%). The initial stage of the investigation of Internet fraud, depending on the content of the initial information, is characterized by situations determined by the presence (80%) or absence (17.5%) of identified digital footprints in conjunction with the establishment of the method of committing a crime, victims and witnesses, the lack of information about the fraudster. A far less likely situation is characterized by the establishment of digital footprints, the method of committing a crime, victims and witnesses, the presence of some information on the criminal, but the lack of data about his/her location (2.5%). Three typical situations of the subsequent stage of the investigation of these crimes are classified depending on the degree of the confession of guilt by the accused and the sufficiency of evidence. The most common situation is characterized by the confession of guilt by the accused and the availability of necessary evidence in the case (90%). In each typical situation, the algorithm of the investigator's actions is determined, methodological recommendations on the tactics of individual investigative actions are developed taking into account the specifics of the crimes committed. Particular attention is paid to the issues of working with digital footprints, the necessary software and hardware are indicated; to the features of the tactics of inspecting the scene, mobile and computer devices; to the determination of the issues to be clarified during the interrogation of the accused, victims, witnesses.

**REFERENCES**

1. Ministry of Internal Affairs of the Russian Federation. (2019) *Brief description of the state of crime in the Russian Federation for January-December 2019*. [Online] Available from: https://xn--b1aew.xn--p1ai/reports/item/19412450/ (Accessed: 29.02.2020). (In Russian).
2. Russia Today. (2019) *V MVD otsenili ushcherb ot kiberprestupleniy v Rossii v 2019 godu* [The Ministry of Internal Affairs assessed the damage from cybercrimes in Russia in 2019]. [Online] Available from: https://Russian.rt.com/russia/ news/696185-mvd-kiberprestuplenie-statistika (Accessed: 29.02.2020).
3. Volchetskaya, T.S. (1997) *Kriminalisticheskaya situalogiya* [Forensic situation studies]. Moscow: Kaliningrad.
4. Ushakov, D.N. (2014) *Tolkovyy slovar' sovremennogo russkogo yazyka* [Explanatory dictionary of the modern Russian language]. Moscow: Adelant.
5. Ministry of Internal Affairs of the Russian Federation. (2016) *In Ivanovo Oblast, the police uncovered a series of Internet frauds.* [Online] Available from: https://xn--b1aew.xn--p1ai/news/item/8984038 (Accessed: 12.07.2019). (In Russian).
6. Kolycheva, A.N. (2018) *Fiksatsiya dokazatel'stvennoy informatsii, khranyashcheysya na resursakh seti Internet* [Fixation of evidentiary information stored on the resources of the Internet]. Law Cand. Diss. Moscow.
7. Judicial and regulatory acts of the Russian Federation. (2019) *Sentence of the Leninsky District Court of Tyumen No. 1-20/2019 1-718/2018 of 16 May 2019 in Case No. 1-20/2019.* [Online] Available from: https://sudact.ru/regular/doc/HxP89erYhSxq/?regular-txt=&regular-case_doc=1-20%2F2019&regular-lawchunkinfo=&regular-date_from=01.05.2019&regular-date_to= (Accessed: 12.07.2019). (In Russian).
8. RF MIA Office for Ivanovo Oblast. (2019) *Report of Police Colonel V.A. Pronin, the Acting Chief of the RF MIA Office for Ivanovo Oblast, to the deputies of Ivanovo Regional Duma, March 28, 2019*. [Online] Available from: https://37.xn--b1aew.xn--p1ai/%D0%BE%D1%82%D1%87%D0%B5%D1%82-%D0%BD%D0%B0%D1%87%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%BA%D0%B0-%D1%83%D0%BC%D0%B2%D0%B4-%D1%80%D0%BE%D1%81%D1%81%D0%B8%D0%B8-%D0%BF%D0%BE-%D0%B8%D0%B2%D0%B0%D0%BD%D0%BE%D0%B2%D1%81%D0%BA (Accessed: 12.07.2019). (In Russian).
9. Alekseeva, T.A., Akhmedshin, R.L. & Yuan', V.L. (2018) Issledovanie lichnosti obvinyaemogo posredstvom analiza materiala sotsial'nykh setey [Investigation of the personality of the accused by analyzing social network data]. In: Davydov, S.I. & Polyakov, V.V. (eds) *Ugolovno-protsessual'nye i kriminalisticheskie chteniya na Altae: problemy i perspektivy protivodeystviya prestupleniyam, sovershaemym s primeneniem informatsionnykh tekhnologiy* [Criminal-procedural and criminalistic readings in Altai: Problems and prospects of countering crimes committed with the use of information technologies]. Vol. 15. Barnaul: Altai State University. pp. 7–14.
10. Shevchenko, E.S. (2016) Social and technological determinants of investigative activities in investigating cyber crimes. *Aktual'nye problemy rossiyskogo prava – Actual Problems of Russian Law*. 10 (71). pp. 160–169. (In Russian). DOI: 10.17803/1994-1471.2016.71.10.160-169
11. Akhmedshin, R.L. (2011) Some psychological aspects of carrying out a search. *Vestnik Tomskogo gosudarstvennogo universiteta – Tomsk State University Journal*. 348. pp. 82–85. (In Russian).
12. Polyakov, V.V. & Shiryaev, A.V. (2015) Problemy taktiki doprosa po delam o komp'yuternykh prestupleniyakh [Problems of interrogation tactics in cases of computer crimes]. *Aktual'nye problemy bor'by s prestupleniyami i inymi pravonarusheniyami*. 15-1. pp. 123–126.

Received: 24 September 2020