УГОЛОВНО-ПРАВОВЫЕ НАУКИ

Научная статья
УДК: 343.9

АКТУАЛЬНЫЕ АСПЕКТЫ ПРОВЕДЕНИЯ ОБЫСКА И СЛЕДСТВЕННОГО ОСМОТРА ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Хачатур Ашотович Асатрян[1], Анна Александровна Христюк[2]
[1,2]Байкальский государственный университет, г. Иркутск, Российская Федерация
[1]AsatryanHA@bgu.ru
[2]KhristukAA@bgu.ru

Аннотация. В последние годы рост преступлений, совершенных с использованием современных информационных и телекоммуникационных технологий, стремительно увеличивается. Информационный этап развития общества приводит к модернизации всех его процессов, в том числе способов совершения преступлений, что определяет необходимость совершенствовать производство следственных действий. В статье авторами рассматривается проблема проведения следственных действий в сфере информационно-телекоммуникационных технологий и предлагаются рекомендации по их разрешению.

Ключевые слова: обыск, осмотр, IT-преступления, киберпреступления, расследование преступлений, электронные следы

Для цитирования: Асатрян, Х. А., Христюк, А. А. Актуальные аспекты проведения обыска и следственного осмотра при расследовании преступлений, совершенных с использованием современных информационных и телекоммуникационных технологий // Криминалистика: вчера, сегодня, завтра. 2025. Т. 35. № 3. С. 7–18.

CURRENT ASPECTS OF CONDUCTING SEARCHES AND INVESTIGATIVE INSPECTIONS DURING THE INVESTIGATION OF CRIMES COMMITTED USING MODERN INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Khachatur Ash. Asatryan[1], Anna A. Khristyuk[2]
[1,2]Baikal State University, Irkutsk, Russian Federation
[1]AsatryanHA@bgu.ru
[2]KhristukAA@bgu.ru

Abstract. In recent years, the number of crimes committed using modern information and telecommunications technologies has increased rapidly. The information stage of society's development leads to the modernization of all its processes, including the methods of committing crimes, which determines the need to improve the production of investigative actions. In this article, the authors examine the problem of conducting investigative actions in the field of information and telecommunications technologies and offer recommendations for their resolution.

Keywords: search, inspection, IT crimes, cybercrimes, crime investigation, electronic traces

For citation: Asatryan Kh. A., Khristyuk A. A. Aktual'nyye aspekty provedeniya obyska i sledstvennogo osmotra pri rassledovanii prestupleniy, sovershennykh s ispol'zovaniyem sovremennykh informatsionnykh i telekommunikatsionnykh tekhnologiy [Current aspects of conducting a search and investigative inspection during the investigation of crimes committed using modern information and telecommunication technologies]. Kriminalistika: vchera, segodnya, zavtra = Forensics: yesterday, today, tomorrow. 2025, vol.35 no. 3, pp. 7–18 (in Russ.).

Введение

Эффективное расследование преступлений, совершенных с использованием информационных технологий, прежде всего принадлежит невербальным следственным (розыскным) действиям, в результате проведения которых следователь самостоятельно получает информацию, находящуюся на объектах материального мира. Такими следственными действиями могут быть обыск и следственный осмотр.

Основная часть

Обыск производится при наличии к нему оснований, предусмотренных ст. 182 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ)[1]. Он может быть произведен не только у подозреваемого, обвиняемого, но и у других лиц, у которых предполагается наличие любых вещей, предметов, имеющих значение для дела. У подозреваемого он проводится в обязательном порядке, независимо от времени совершения преступления [1, с. 6].

Современные способы совершения преступлений характеризуются не только непосредственным использованием информационных технологий, но и использованием электронных сообщения для внутреннего взаимодействия, напраимер отправка и передача информации о предмете посягательства, а также в отдельных случаях общение между потерпевшим и преступником осуществляются в электронной форме, в частности посредством средств информационных, телекоммуникационных, информационно-телекоммуникационных систем. Для выявления таких электронных сообщений, важное место принадлежит обыску.

[1] Уголовно-процессуальный кодекс Российской Федерации : УПК : принят Гос. Думой 21 ноября 2001 года : одобрен Советом Федерации 5 декабря 2001 года : послед. ред. // КонсультатнтПлюс : сайт. URL: https//www.consuitant.ru/document/cons_doc_LAW_34481/ (дата обращения: 07.08.2025).

На подготовительном этапе проведения обыска необходимо установить:

– количество объектов, на которых будет производиться обыск, и их точный адрес. Например, лица могут совершать мошеннические действия с использованием информационных технологий из разных объектах;

– какие предметы подлежат обыску;

– пути подхода и способы проникновения в помещение, подлежащие обыску;

– количество лиц, проживающих (работающих) в помещении;

– обеспечить целостность и охрану места проведения обыска.

Необходимо отметить, что организация и проведение обыска в уголовных производствах о преступлениях, совершаемых с использованием информационных технологий, отличаются от обыска при расследовании традиционных видов преступлений. Это обусловлено опасностью быстрого умышленного уничтожения электронных носителей и информации, хранящейся на них, имеющей доказательное значение. Кроме того, информация может быть уничтожена или повреждена неосторожным поведением следователя и других членов следственно-оперативной группы, которые также могут уничтожить информационные следы в результате неправильного, неквалифицированного обращения с информационными технологиями [2, с. 59].

В связи с этим при подготовке к обыску непосредственно на месте предполагаемого преступления с использованием информационных технологий проводятся следующие мероприятия:

– получение информации о предметах, подлежащих обнаружению: информационных технологий (стационарный компьютер, ноутбук, сервер и т. п.), программное обеспечение и носители информации, которые необходимо изъять и т. д.;

– приглашение специалистов-экспертов компьютерно-технического отдела экспертно-криминалистической службы МВД России или сотрудников управления по борьбе с противоправным использованием информационно-коммуникационных технологий МВД России (УБК МВД России);

– приглашение понятых, разбирающихся в компьютерной технике;

– подготовка соответствующих устройств и компьютерных средств, которые будут использоваться для считывания и хранения извлекаемой из электронных носителей информации;

– проведение инструктажа членов следственно-оперативной группы (при этом особое внимание следует уделить их действиям при обыске) и других участников обыска (строгое соблюдение установленных правил обращения с компьютерной техникой и носителями информации, технически грамотное проведение поиска доказательств, нужной информации).

Таким образом, во время подготовки к проведению обыска, а также в целях получения помощи при производстве обыска по вопросам, требующим специальных знаний, следователь может поручить оперативным сотрудникам, как правило, из управления по борьбе с противоправным использованием информационно-коммуникационных тех-

нологий МВД России или уголовного розыска собрать необходимые сведения об объекте и помещении, где планируется осуществить обыск.

Вместе с тем необходимо определить, какие объекты находятся рядом, а также последовательность, способ и границы обыска, исследовать весь комплекс вопросов, относящихся к обстоятельствам преступления, определить взаимное расположение и взаимосвязь элементов обстановки, обратить внимание на состояние предметов, объектов, которые будут рядом.

Целью обыска места совершения преступлений, совершенных с использованием информационных технологий, является: изучение и фиксация обстановки места происшествия, выявление, фиксация и изъятие следов преступления и вещественных доказательств, выявление преступника и уяснение его мотивов, выдвижение версий о произошедшем, получение данных о лицах, которые могли знать о совершении преступления, с целью организации проведения других следственных (розыскных) действий [3, с. 77].

Объекты обыска при совершении преступлений с использованием информационных технологий условно можно разделить на следующие виды, а именно:

1. Указывающие на принадлежность информационных технологий к совершению преступления:

– оперативно запоминающее устройство (компьютеры, их системные блоки, внешние накопители информации);

– периферийные устройства (мониторы, принтеры, дисководы, модемы, сканеры, клавиатуры, манипуляторы, джойстики и др.), коммуникационные приборы компьютеров и вычислительных сетей;

– носители информации (жесткие диски, флоппи-диски, оптические диски, флэш-память, внешние и внутренние диски (HDD, SSD и т. п.);

– распечатка программных и текстовых файлов;

2. Указывающие на принадлежность определенного лица к совершению преступления:

– электронные записные книжки, другие электронные носители текстовой или цифровой информации, техническая документация к ним;

– отпечатки пальцев рук на периферийных устройствах, носителях информации и других предметах, которые использовались для совершения преступлений;

– предметы, полученные в результате совершения уголовного правонарушения (вещи, деньги, другое имущество).

В зависимости от особенностей помещения обыск может быть следующих видов: концентрический (по спирали – от периферии к центру), эксцентричный (по спирали – от центра к периферии), фронтальный (исследование объекта средствами, которые расположены в линию и перемещаются фронтально), по квадратам (помещение или территория делится на обыскиваемые поочередно квадраты), по секторам (за основу берется точка, от которой по кругу производится обыск по секторам: от 30° до 45°).

При обыске необходимо производить фотографирование и видеозапись, в частности с использованием фототаблиц. По мнению Д. Н. Маринкина, положительным

фактором, во многом предупреждающим возможные попытки совершения противодействия со стороны преступников, является использование в процессе обыска видеосъемки. Ее наличие позволит зафиксировать: во-первых, непосредственно сам факт обнаружения предметов, во-вторых, соблюдение всех процессуальных правил проведения следственного действия и грамотность действий членов следственной группы [4, с. 146].

При проведении видеосъемки обыска целесообразно фиксировать окружающую обстановку с помощью фотосъемки с использованием правил узловой и детальной съемки. Все действия должны проводиться специалистом, получившим право проведения осмотра места совершения преступления с использованием информационных технологий, или сотрудником управления по борьбе с противоправным использованием информационно-коммуникационных технологий МВД России.

При проведении обыска и осмотра электронных носителей информации важную роль занимает специалист. Сложившаяся практика демонстрирует возможность успешного осуществления поиска информации без проведения экспертного исследования в рамках проведения осмотра с участием специалиста [5, с. 265].

Начиная осмотр информационных носителей, следователь и специалист должны соблюдать определенные правила с целью обеспечения обнаружения и извлечения вещественных доказательств (следов пальцев рук и объектов биологического происхождения). К особенностям указанного этапа необходимо отнести:

– отображение следов пальцев рук нужно искать на клавиатуре компьютера, манипуляторе типа «мышь», устройствах сменных накопителей данных;

– следы, образующиеся при подключении аппаратуры, с помощью которой осуществляется несанкционированное копирование информации системного блока, к сети [6, с. 36];

– выявление объектов биологического происхождения (например, волосы), которые могут в дальнейшем служить доказательствами в уголовном производстве, а именно: на информационных носителях, периферийных устройствах (принтер, сканер, клавиатура, мышка, многофункциональное устройство, блок непрерывного питания, накопители памяти, роутер и т. п.), рабочем месте (стол, стул, пол, коврик для мыши, другие предметы, находящиеся рядом), одежде и т. д.

Извлекать нужно все носители информации (накопители памяти – DVD и CD-диски, флэш-карты, SSD, HDD и т. д.). Провести тщательный обзор документации, обращая особое внимание на рабочие записи операторов, так как часто именно в этих записях пользователей можно найти коды, пароли и другую полезную для доказывания вины информацию. При наличии возможности непосредственного доступа к компьютеру и отсутствии всех нежелательных ситуаций следователь и специалист приступают к его осмотру. При этом все свои действия следователи и специалисты должны четко разъяснять понятым.

Требуется установить наличие у компьютера внешних устройств

удаленного доступа к системе (подключение к локальной сети, наличие модема). По возможности необходимо произвести точную информационную копию машинного носителя. Если во время обыска обнаруживаются другие предметы и документы, они обязательно предъявляются понятым.

Важным этапом в проведении обыска является фиксирование его результатов, а именно составление протокола. Надлежащее оформление источника фактических данных, в частности протокола процессуального действия, предусмотрено ст. 166 УПК РФ, согласно которой ход и результаты проведения процессуального действия фиксируются в протоколе. Последний должен содержать не только результаты процессуального действия, но и описание его течения.

Описательная часть протокола должна содержать сведения об общей характеристике места проведения обыска, а также информацию о границах, подвергнутых обыску территории или помещения. Описываются также пути подхода к объекту обыска (при необходимости) относительно самого места обыска – состояние входов, смежных помещений, лестниц, дверей, окон, замков. В протоколе предметы описываются последовательно, как были обнаружены и осмотрены, и в том виде, в каком находились на момент их обнаружения.

При возможности (если следователям удалось это установить) указывается конфигурация компьютера с четким описанием всех комплектующих и устройств, отмечаются названия моделей и серийные номера каждого из устройств, если они нанесены на эти устройства: серийный номер – Serial Number, Serial N или S/N и другая информация с заводских наклеек, а также имеющиеся инвентарные номера, присваиваемые бухгалтерией при постановке оборудования на баланс предприятия (при наличии таковых).

В протоколе должны использоваться только однозначные слова и выражения, употребляемые в сфере компьютерных технологий. Необходимо избегать жаргонных слов, обозначающих упомянутые предметы, а также сокращенных слов и словосочетаний, используемых в обычном языке для обозначения компьютерной техники.

В случае обнаружения следов пальцев рук в протоколе обыска следует описать: место их обнаружения (на каких предметах они найдены, где эти предметы находились на месте уголовного правонарушения, название и назначение предметов), количество следов и их расположение (расстояние от двух неподвижных ориентиров), описание поверхности предмета (стекло, бумага, металл, древесина, пластмасса, окрашенная, непокрашенная, никелированная, полированная, разноцветная и т. п.), состояние поверхности предмета (сухая, влажная, маслянистая, загрязненная, покрытая пылью), вид следов (потожировые, окрашенные, рельефные, слабовидимые, невидимые), при возможности определения – тип узора (дуговой, петлевой, завиточный), форма и размер следа (максимальная длина и ширина), способ обнаружения (визуальный, окрас порошками или парами йода и т. п.), способ извлечения при фиксации (сам предмет или его часть вместе со следом, фотографирование, ко-

пирование на пленку, изготовление слепка, материал слепка), как упакован и какой печатью опечатывались вещественные доказательства.

При необходимости дополнительно фотографируют обнаруженные предметы и следы. С этой целью у каждого предмета расставляются соответствующие цифровые бирки и масштабные линейки (метрики), свидетельствующие о размере предметов. Цифры должны находиться у каждого предмета и не повторяться. При этом следователь может использовать смартфон для фиксации следов преступления, составления фототаблиц, планов, чертежей и схем [7, с. 24]. Например, в мобильном приложении «CrimLib.info – Справочник следователя» размещена полезная информация для следователей – мультиспектральная система экспертного света, позволяющая запечатлевать объекты в высоком разрешении [8, с. 201].

В конце протокола приводятся все заявления и замечания понятых и участников обыска по тем или иным действиям следователя. При отсутствии замечаний в протоколе делается соответствующая отметка, Оба экземпляра протокола, а также описание изъятых предметов подписывают следователь, лицо, у которого проводился обыск, и приглашенные присутствовавшие. Если в ходе обыска были сделаны попытки уничтожить или скрыть определенные предметы или документы, подлежащие изъятию, то об этом в протоколе делается соответствующая запись и указываются принимаемые меры.

После описания изъятые предметы и документы упаковываются и опечатываются. Для сохранения следов преступления изъятая электронная техника опечатывается с соблюдением следующих правил. Необходимо ее отключить от сети, отсоединить разъемы и наложить на них лист бумаги, закрепляя его края на боковых стенках компьютера густым клеем или клейкой лентой для того, чтобы исключить возможность работы с ним в отсутствие следователя или эксперта. Также необходимо опечатать все составляющие информационных технологий бумажными лентами, на которых ставятся подписи следователя, специалиста, понятых, номер ЭВМ. Для приклеивания используется липкая лента, которую крепят таким образом, чтобы при попытке снять ее нарушилась целостность бумаги с подписями. Аналогично опечатываются разъемы (кабели) с соблюдением соответствия номеров на разъеме блока компьютера и соединительных проводах.

Обыску подлежат находящиеся в помещении лица и их личные вещи. При таких обстоятельствах возможно изъятие других предметов, которые могут стать вещественными доказательствами.

Специфика обзора информации состоит в следующем:

1) компьютерная информация является специфическим объектом поиска;

2) обследование информационных технологий и носителей информации может приобретать самостоятельное значение;

3) не всегда есть возможность в изъятии информационных технологий, отдельных их комплектующих, чтобы с помощью других действий зафиксировать и исследовать информацию;

4) обследование информационных технологий и ее носителей всегда предполагает необходимость приглашения соответствующего специалиста в области компьютерных технологий, компьютерных систем и т. п.;

5) информационные технологии получают все большее распространение, существуют разнообразные программы защиты и экстренного уничтожения информации.

После наружного осмотра следователь и специалист приступают к внутреннему осмотру системного блока. Это связано с необходимостью подтверждения установки в компьютерной технике устройств, плат и другого оборудования, их расположения внутри системного блока, выявления новых, не определенных внешним осмотром устройств и плат (особенно отмечается наличие неизвестных ему устройств, например, для уничтожения информации). При внутреннем осмотре устанавливаются индивидуальные признаки устройств и плат, их серийные номера.

В случае необходимости из информации, находящейся в памяти компьютерной техники, производится копия на HDD, принадлежащая экспертному подразделению или правоохранительному органу. Если при обзоре компьютерной техники возникли проблемы с ее запуском, открытием и просмотром отдельных программ, то в данном случае осуществляется обзор тех ресурсов (программ, файлов), которые позволяет оперативное запоминающее устройство.

При осмотре компьютерной техники с целью дальнейшего отображения в протоколе специалисты должны обращать внимание на следующее:

а) электронную переписку, в том числе с потерпевшим (когда был создан сайт, логин и пароль, исходящую и входящую корреспонденцию с потерпевшим и интернет-ресурсы, задействованные до совершения преступления);

б) личный кабинет на сайтах объявлений (например, Avito, «ВКонтакте», «Телеграм») – когда, кем была создана учетная запись, ее название, логин и пароль, кому принадлежит личный кабинет, какой телефон к нему подключен, когда осуществлялись в него вхождения, какие сообщения были размещены по указанной учетной записи, какие изменения были произведены, в какое время и т. п.);

в) осуществляется обзор социальных сетей. Обзору подлежит профиль социальной страницы, когда, кем он был создан, его название, логин и пароль, какой телефон к нему подключен, какие сообщения, фотографии, видеоконтент размещены на профиле и т. п.;

г) обнаруживаются и просматриваются файлы, в том числе фотографии, которые были отображением предмета посягательства при совершении преступлений с использованием компьютерной техники (например, фотография транспортного средства, за которое потерпевший уплатил денежные средства). Учитывая, что указанные файлы могли быть размещены сначала на компьютерной технике после загрузки с телефона или сети Интернет, они оставляют соответствующие электронные следы, а именно дату их создания или удаления;

д) просматривают личный кабинет интернет-банкинга, когда, кем были они созданы, какая у них учетная запись, на кого они зарегистрированы, их название, логин и пароль, кому принадлежит, какой телефон к ним подключен, какие и когда осуществлялись операции по ним, в частности, по получению средств от потерпевшего;

е) просматриваются другие данные, в частности названия и версии программ, которые установлены и могут являться доказательствами совершения преступления с использованием информационных технологий.

Осуществляя обзор веб-страницы, следователь должен ее масштабировать в полный размер (100 %). В браузере должны быть отключены все приложения и надстройки, которые могут изменить вид веб-страницы, категория или жанр публикации, если они указаны на веб-странице, публикации, основной текст публикации, аудио- или видеофайлы. В дальнейшем рекомендуется осуществить печать веб-страниц, личных кабинетов, электронной переписки, профилей в интернет-ресурсах и добавить в протокол осмотрап как неотъемлемое приложение с указанием серийного номера, названия и модели принтера, где печаталась такая информация. Фото-, видео- и аудиофайлы, являющиеся частью публикации, должны быть сохранены и записаны на диск. Альтернативным средством фиксации веб-страницы является сохранение ее в формате html-средствами программы-браузера с последующей записью такого файла на диск.

Выводы и заключение

Обыск и осмотр при расследовании преступлений, совершенных с использованием информационных технологий, являются одними из наиболее сложных, объемных и информационно значимых, от качества проведения которых зависит успех дальнейшего расследования IT-преступлений. Именно поэтому соблюдение приведенных выше практических рекомендаций по вопросам проведения обыска и осмотра имеет важное значение. В заключение хочется отметить, что большинство экспертов прогнозируют увеличение числа преступлений с использованием современных компьютерных технологий [9–12]. В связи с этим правоприменительным органам необходимо разработать актуальные методы предупреждения, обнаружения, фиксации и противодействия преступлениям в этой сфере.

СПИСОК ИСТОЧНИКОВ

1. *Бадзгарадзе, Г. Д.* Особенности возбуждения уголовного дела о мошенничестве, совершенном с использованием информационных технологий // Криминалистъ. 2023. № 3 (44). С. 3–10.

2. *Ревенко, Н. И.* Материальные и электронно-цифровые следы как элемент криминалистической характеристики мошенничеств, совершенных способом «Ваш родственник попал в беду» // Юридические исследования. 2024. № 8. С. 58–64.

3. *Ковалик, Б. В.* Теоретические аспекты выявления и раскрытия мошенничеств, совершенных с использованием информационно-коммуникационных технологий и методов социальной инженерии // Юстиция Беларуси. 2024. № 9 (270). С. 45–49.

4. *Маринкин, Д. Н.* Особенности первоначального этапа расследования мошенничества с финансовой пирамидой, совершенного с использованием информационных технологий блокчейн // Аграрное и земельное право. 2019. № 2 (170). С. 145–147.

5. *Себякин, А. Г.* Возможности использования контекстного поиска информации на компьютерных носителях в целях выявления, расследования и профилактики преступлений // Всероссийский криминологический журнал. 2019. Т.13. № 2. С. 262–270.

6. Цифровые следы преступлений : монография. М. : Проспект, 2021. 168 с.

7. *Ищенко, Е. П.* У истоков цифровой криминалистики // Вестник университета им. О. Е. Кутафина. 2019. № 3. С. 15–28.

8. *Ищенко, Е. П., Кручинина, Н. В.* Высокие технологии и криминальные вызовы // Всероссийский криминологический журнал. 2022. Т. 16. № 2. С. 199–206.

9. *Фойгель, Е. И., Проценко, А. Г.* К вопросу о проблемах практической реализации нового оперативно-розыскного мероприятия «получение компьютерной информации» при раскрытии преступлений в сфере компьютерной информации // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. № 6 (14). С. 73–82.

10. *Валькирия, Н. И.* Общая теория криминалистики в эпоху развития цифровых технологий: некоторые актуальные проблемы // Сибирские уголовно-процессуальные и криминалистические чтения. 2024. № 4 (46). С. 15–25.

11. *Степаненко, Д. А.* Киберпространство как модулятор процесса расследования преступлений и развития криминалистической науки // Сибирские уголовно-процессуальные и криминалистические чтения. 2020. № 1. С. 77–88.

12. *Коломинов, В. В.* Мошенничество в сфере компьютерной информации: криминалистический аспект // Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права). 2015. Т. 6. № 1. С. 153–160.

REFERENCES

1. *Badzgaradze, G. D.* Osobennosti vozbuzhdeniya ugolovnogo dela o moshennichestve, sovershennom s ispol'zovaniyem informatsionnykh tekhnologiy [Features of Initiating a Criminal Case for Fraud Committed with the Use of Information Technology]. Kriminalist – Kriminalist. 2023. no. 3 (44). Pp. 3–10 (in Russian)

2. *Revenko, N. I.* Material'nyye i elektronno-tsifrovyye sledy kak element kriminalisticheskoy kharakteristiki moshennichestv, sovershennykh sposobom «Vash rodstvennik popal v bedu» [Material and Electronic-Digital Traces as an Element of the Forensic Characteristics of Frauds Committed by the "Your Relative is in Trouble" Method]. Yuridicheskiye issledovaniya – Legal Research. 2024. no. 8. Pp. 58–64. (in Russian)

3. *Kovalik, B.V.* Teoreticheskiye aspekty vyyavleniya i raskrytiya moshennichestv, sovershennykh s ispol'zovaniyem informatsionno-kommunikatsionnykh tekhnologiy i metodov sotsial'noy inzhenerii [Theoretical aspects of identifying and exposing fraud committed using information and communication technologies and social engineering methods]. Yustitsiya Belarusi. – Justice of Belarus. 2024. no. 9 (270). Pp. 45–49. (in Russian)

4. *Marinkin, D. N.* Osobennosti pervonachal'nogo etapa rassledovaniya moshennichestva s finansovoy piramidoy, sovershennogo s ispol'zovaniyem informatsionnykh tekhnologiy blokcheyn [Features of the initial stage of the investigation of fraud with a financial pyramid committed using blockchain information technologies]. Agrarnoye i zemel'noye pravo. – Agrarian and Land Law. 2019. no. 2 (170). Pp. 145–147. (in Russian)

5. *Sebyakin, A. G.* Vozmozhnosti ispol'zovaniya kontekstnogo poiska informatsii na komp'yuternykh nositelyakh v tselyakh vyyavleniya, rassledovaniya i profilaktiki prestupleniy [Possibilities of using contextual search of information on computer media for the purpose of identifying, investigating and preventing crimes]. Vserossiyskiy kriminologicheskiy zhurnal – All-Russian Criminological Journal. 2019. Vol. 13. no. 2. Pp. 262–270. (in Russian)

6. Tsifrovyye sledy prestupleniy : monografiya [Digital Traces of Crimes: A Monograph]. Moscow: Prospect, 2021. 168 p. (in Russian)

7. *Ishchenko, E. P.* U istokov tsifrovoy kriminalistiki [At the Origins of Digital Forensics]. Vestnik universiteta im. O. Ye. Kutafina. – Vestnik of the Kutafin University. 2019. no. 3. Pp. 15–28. (in Russian)

8. *Ishchenko, E. P., Kruchinina, N. V.* Vysokiye tekhnologii i kriminal'nyye vyzovy [High Technologies and Criminal Challenges]. Vserossiyskiy kriminologicheskiy zhurnal. – All-Russian Criminological Journal. 2022. Vol. 16. no. 2. Pp. 199–206. (in Russian)

9. *Foigel, E. I., Protsenko, A. G.* K voprosu o problemakh prakticheskoy realizatsii novogo operativno-rozysknogo meropriyatiya «polucheniye komp'yuternoy informatsii» pri raskrytii prestupleniy v sfere komp'yuternoy informatsii [On the issues of practical implementation of the new operational-search measure "obtaining computer information" in solving crimes in the sphere of computer information]. Sibirskiye ugolovno-protsessual'nyye i kriminalisticheskiye chteniya. – Siberian criminal procedure and forensic readings. 2016. no. 6 (14). Pp. 73–82. (in Russian)

10. *Valkyrie, N. I.* Obshchaya teoriya kriminalistiki v epokhu razvitiya tsifrovykh tekhnologiy: nekotoryye aktual'nyye problem [General Theory of Forensic Science in the Age of Digital Technologies: Some Current Issues]. Sibirskiye ugolovno-protsessual'nyye i kriminalisticheskiye chteniya. – Siberian Criminal Procedure and Forensic Readings. 2024. no. 4 (46). Pp. 15–25. (in Russian)

11. *Stepanenko, D. A.* Cyberspace as a Modulator of the Crime Investigation Process and the Development of Forensic Science [Kiberprostranstvo kak modulyator protsessa rassledovaniya prestupleniy i razvitiya kriminalisticheskoy nauki]. Sibirskiye ugolovno-protsessual'nyye i kriminalisticheskiye chteniya – Siberian Criminal Procedure and Forensic Science Readings. 2020. no. 1. Pp. 77–88. (in Russian)

12. *Kolomin, V. V.* Moshennichestvo v sfere komp'yuternoy informatsii: kriminalisticheskiy aspect [Fraud in the field of computer information: forensic aspect]. Bulletin of the Irkutsk State University of Economics (Baikal State University of Economics and Law). 2015. Vol. 6. no. 1. Pp. 153–160. (in Russian)

ИНФОРМАЦИЯ ОБ АВТОРАХ

Асатрян Хачатур Ашотович, кандидат юридических наук, доцент, доцент кафедры криминалистики, судебных экспертиз и юридической психологии. Байкальский государственный университет. 664003, Российская Федерация, г. Иркутск, ул. Ленина, 11.

Христюк Анна Александровна, кандидат юридических наук, доцент, доцент кафедры уголовного права и криминологии. Байкальский государственный университет. 664003, Российская Федерация, г. Иркутск, ул. Ленина, 11.

INFORMATION ABOUT THE AUTHORS

Khachatur A Asatryan, Candidate of Law Sciences, Associate Professor, Associate Professor of the Department of Criminalistics, Forensic Expertise and Legal Psychology. Baikal State University. 11 Lenina St., Irkutsk, Russian Federation, 664003.

Anna A. Khristyuk, Candidate of Law Sciences, Associate Professor, Associate Professor of the Department of Criminal Law and Criminology. Baikal State University. 11 Lenina St., Irkutsk, Russian Federation, 664003.