А.Б. Смушкин

ОНЛАЙН-ИГРЫ КАК ПРОСТРАНСТВО СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ

Рассматривается компьютерное пространство онлайн-игр как инцидентное пространство совершения преступлений. В ходе анализа специфики преступлений, связанных с инцидентным игровым компьютерным онлайн-пространством с учетом отдельных вопросов игровой механики, экономики и социологии, констатируется необходимость уделять внимание правильному выявлению и квалификации преступлений данной категории, а также предлагаются основы комплексной методики расследования преступлений, связанных с онлайн-играми.

Ключевые слова: ММОРИГ; инцидентное компьютерное пространство; игровая экономика; продажа игровых объектов; осмотр электронного объекта; расследование преступлений, совершенных с использованием онлайн-игр.

Особенностью современного общества можно назвать активную его «виртуализацию». На настоящий момент ситуация позволяет констатировать переход ощутимой части общественной жизни в «виртуальность». А с развитием устройств виртуальной и дополненной реальности будет развиваться и замещение реальной жизни более яркой – виртуальной.

При этом криминалистическим исследованиям онлайн-игр уделяется недопустимо мало внимания. Между тем киберпространство онлайн-игр все чаще становится инцидентным пространством обсуждения, подготовки и совершения преступлений. В инцидентном пространстве онлайн-игр, а также с их использованием может совершаться широкий спектр преступлений. Кроме того, игровое пространство может служить и способом сокрытия преступлений, когда подозреваемый заявляет о наличии у него цифрового алиби.

Специфика игровых миров позволяет выявить возможность совершения в их рамках следующих преступлений и административных правонарушений: разглашения информации с ограничением доступа (государственной тайны, коммерческой и т.д.), публикации экстремистской информации; использования чатов для выдвижения требований при вымогательстве; преступления коррупционного характера; мошенничества в сфере компьютерной информации, вымогательства, неправомерного доступа к компьютерной информации и т.д.

Безусловно, специфика инцидентного пространства приводит к тому, что многие игроки в силу возраста не подлежат привлечению к уголовной ответственности. Однако в онлайн-игры играет и совершеннолетняя молодежь, и люди среднего возраста, и некоторые представители старшего поколения.

Таким образом, применительно к виртуальным мирам правовые отношения приобретают новые свойства и характерные черты, совершенно не присущие традиционным правоотношениям, возникающим в реальном, физическом мире [1. С. 146].

В рамках криминалистической характеристики деянного можно выделить специфику потерпевших, лиц, совершающих преступления, способов совершения преступлений, непосредственного предмета преступления и следовой картины.

Расследование преступлений, связанных с онлайн-играми, осложняет ряд факторов: многие серверы и пользователи онлайн-игр расположены за пределами

РФ, что осложняет взаимодействие с правообладателями и получение информации; затруднена идентификация конкретных пользователей; игроки – это специфическое сообщество, своеобразный узкий круг общения, не стремящийся допустить выхода информации за его пределы. Важно отметить, что сотрудники правоохранительных органов чаще всего недооценивают преступления, совершенные в инцидентном компьютерном пространстве онлайн-игр и зачастую не имеют достаточных знаний и навыков расследования преступлений в такой специфической сфере. Недооценка совершенных деяний выражается, в первую очередь, в том, что преступления, связанные с игровым пространством и игровыми объектами, не воспринимаются как что-то серьезное, как деяния, наносящие реальный материальный ущерб, что чаще всего влечет отказ в возбуждении уголовного дела в связи с отсутствием состава преступления. Между тем 38% опрошенных игроков отметили совершение в отношении них преступлений с использованием игрового инцидентного пространства или в его рамках. Однако сколько-нибудь разработанная методика расследования подобной группы преступлений отсутствует.

Также в качестве способа следует отметить, что почти в любой многопользовательской игре есть мировые чаты игры, чаты «локации», гильдии, клана или конкретной команды, а также чаты личного диалога, в которых могут происходить определенные преступные контакты. Игроки зачастую используют также программы для голосового общения типа Team Speak, RaidCall и др. При этом, данные коммуникационные пространства не контролируются (в большинстве случаев) ни администрациями игр, ни, тем более, правоохранительными органами. Им не уделяется особого внимания при осуществлении получения компьютерной информации, прослушивании телефонных и иных переговоров. К тому же в том объеме трафика, который генерирует крупная многопользовательская игра, не всегда возможно отслеживать в реальном времени коммуникации конкретного игрока. Между тем эти чаты могут служить полем обсуждения преступления или его подготовки, а также непосредственно самого совершения. Как верно отметил О.И. Шиндин, «конечно, с помощью программных фильтров можно выявить отдельные диалоги по ключевым словам, но при этом следует учитывать, что участники корруп-

ционных схем и не будут говорить “прямым текстом”. Все участники могут использовать кодовые слова и обороты для маскировки настоящего смысла диалога» [2. С. 84].

Криминалистически значимая специфика способа совершения преступлений закономерно влечет и специфику следовой картины содеянного. «Классические» трасологические следы для данной категории преступлений менее характерны, чем электронные [3. С. 201–209] – следы в памяти информационно-технологических устройств. Данную группу следов часто в науке именуют и иными терминами: электронно-цифровые [4. С. 64–71], виртуальные [5. С. 85–87; 6], цифровые [7. С. 206], компьютерно-технические [8. С. 11], бинарные [9. С. 18]. Особенности работы с указанной категории следов рассмотрены в трудах многих авторов [6; 10. С. 136–139; 11. С. 53–55; 12. С. 18–25; 13. С. 212–216; 14. С. 171–175], поэтому не будем заострять на этом внимание.

Большие финансовые средства, циркулирующие в рамках реально-виртуальной игровой экономики, притягивают и лиц, желающих эти средства незаконно получить. Специфика игровой экономики при этом требует и существенную специфику расследования.

Указанные обстоятельства определяют повышенную значимость разработки основ комплексных криминалистических рекомендаций по выявлению и расследованию преступлений, связанных с инцидентным пространством онлайн-игр. Не претендуя на полномасштабную комплексную методику, хотелось бы предложить ряд криминалистических рекомендаций различного характера.

На начальном этапе расследования преступлений, совершенных в онлайн-играх, могут сложиться следующие ситуации:

1. Пользователь обнаружил совершенное в отношении него преступление и обратился в правоохранительные органы. Данная ситуация характерна для хищения игровых предметов, вымогательства, мошенничества, в редких случаях – при совершении в игре экстремистских преступлений или угроз жизни либо здоровью.

2. Преступление было обнаружено собственником или администрацией игрового проекта. Было проведено первичное исследование инцидента. Такая ситуация характерна для массового взлома аккаунтов, серверов самой игры или сайта игры. Следует заметить, что программисты и системные администраторы игрового проекта, как правило, обладают достаточной квалификацией для пресечения и противодействия атакам на сервер игры, однако внутреннее расследование подобных инцидентов требует компетенций несколько другого порядка и характера. Для подобных действий крупные проекты приглашают специалистов Лаборатории Касперского, Ггоор-IV и аналогичных фирм, оказывающих на коммерческой основе услуги по расследованию компьютерных инцидентов. Представляется важным подчеркнуть налаженное взаимодействие с данными фирмами для безотлагательного получения максимально полного результата их расследования.

3. О совершенном преступлении сообщили посторонние свидетели. Ситуация характерна для преступ-

лений экстремистского характера. К числу таких свидетелей можно отнести как игроков – незаинтересованных свидетелей вербального (текстового или акустического) преступления экстремистского или иного характера, так и лиц, воспринимавших событие через монитор или иной экран пользователя – участника события (родственников, коллег, знакомых и т.д.).

4. Использование онлайн-игры для совершения преступления выявлено правоохранительными органами. Ситуация может быть характерна для отмывания денежных средств через игровую валюту, использование онлайн-игр для коррупционных схем и т.д.

Относительно круга необходимых следственных действий и их тактики можно отметить несколько основополагающих обстоятельств. В случае совершения преступления в играх, связанных с экстремистской деятельностью или подобными преступлениями, отобразившимися в чатах диалогов, наименовании игрока и его клана или иного объединения, возможно провести допрос выявивших данные нарушения и выемку снимков экрана у игроков. Это связано с тем, что игроки достаточно часто сохраняют подобные снимки, скриншоты (от англ. Screenshots) в целях последующего использования в качестве подтверждения своих претензий в игровых диалогах. Участники игр часто не терпят неподтвержденных обвинений, претензий и требуют так называемые пруфы (от англ. Proof – доказательство). Следовательно, велика вероятность того, что игрок сохранит снимок экрана, подтверждающий его слова).

При производстве расследования данной категории преступлений существенную пользу оказало бы действие или мероприятие, проводимое аналогично растровому розыску в Германии, поскольку большинство аккаунтов (учетных записей) “привязано” к странице в социальных сетях либо создает аналог социальной сети на сайте владельца проекта. По словам В.Ю. Сокола, «в процессе растрового розыска компьютерная обработка широкого круга персональных информационных массивов осуществляется с учетом разрабатываемого правоохранительными органами так называемого «профиля» (криминалистической информационной модели предполагаемого преступника), представляющего собой упорядоченный набор поисковых признаков лиц, совершающих данный вид преступлений. В результате обработки баз персональных данных с помощью специальной программы из огромного информационного массива выбираются те субъекты, которые соответствуют составленному растру (профилю, портрету), исключая всех тех, кто не совпадает с заданными критериями» [15. С. 36–37]. С помощью растрового розыска могли бы быть проверены социальные сети для обнаружения не только основного персонажа пользователя-злоумышленника, но и дополнительных (твинов, мультвов).

В рамках расследования данной категории преступлений особую результативность могло бы иметь предложенное нами ранее следственное действие «Осмотр электронного объекта». Как мы указывали, «в рамках следственного действия “Осмотр электронного объекта” возможно выделение следующих подвидов: осмотр локального устройства, сетевой осмотр,

осмотр распределенного объекта (файлы, хранящиеся в облачных сервисах и блокчейны), осмотр мобильного устройства. Осуществляться такой осмотр должен с обязательным привлечением специалиста. При применении специального программного или технического обеспечения об этом делается отметка в протоколе» [16. С. 80]. Относительно фиксации данного следственного действия мы рекомендуем закрепить требование о распечатке и копировании информации, полученной в ходе осмотра электронного объекта, в присутствии понятых и только с помощью сертифицированных программ. В ходе подобного осмотра на локальном устройстве пользователя могут быть обнаружены файлы уголовно-релевантного содержания, аккумулирующие криминалистически значимую информацию: различные записи для памяти, планы. При переписке через мессенджеры и коммуникационные программы типа Discord на устройствах пользователя могут быть сохранены в соответствующих директориях передаваемые файлы картинок, видео- и звукозаписей. Также на компьютере пользователя в ходе осмотра могут быть обнаружены программы-«боты» для имитации диалогов, игровых или иных действий, на манипуляторе типа «игровая мышь» может быть так же обнаружена программа действия. Что касается сетевого осмотра, может быть обнаружен и изучен ряд аккаунтов лица в социальных сетях, с помощью которых проводились мошеннические действия, переписка на форумах и т.д. Осмотру может быть также подвержен электронный кошелек пользователя в системах «Яндекс-деньги», Qiwi, Webmoney и т.д.

При расследовании хищения игровых предметов необходимо учитывать, что если данные предметы покупались пользователями у других пользователей за реальные денежные средства, их стоимость можно определить, проведя выемку выписки со счета, с которого производился перевод, и справки о транзакции. Покупка объекта в игровом магазине может оцениваться с помощью конвертации валюты игрового магазина в объеме стоимости виртуального объекта в реальные денежные средства по курсу, установленному администрацией игры. Кроме того, если для покупки в игровом магазине в игру вводились реальные денежные средства, подтвердить их объем можно в том числе с помощью выемки соответствующих документов, отражающих электронный перевод, а также поступление их на счет организации, владельца компьютерной игры и расходование на игровой процесс. В случае же необходимости оценки предмета заработанного, полученного или купленного с помощью средств, предусмотренных механикой игрового процесса, мы склонны согласиться с рекомендацией В.И. Еремченко и О.В. Сафронкина, призывающих применять в подобной ситуации подход, аналогичный оценке произведений искусства. Как они далее указывают, «вопросы оценки предметов виртуальной собственности должны быть отнесены к компетенции специалистов, непосредственно разрабатывающих и поддерживающих игровой процесс конкретной ММО-игры, так как именно они устанавливают игровой баланс, определяют соотношение цены игровой и реальной валюты. ...Видится логичным отнести подоб-

ные исследования к классу судебно-экономических экспертиз и именовать их судебно-оценочной экспертизой (исследованием) стоимости объектов виртуальной собственности» [17. С. 67].

В ходе расследования рассматриваемой категории преступлений возникает необходимость допроса потерпевшего и свидетелей. При этом представляется необходимым рекомендовать, чтобы следователь, проводящий допрос, хотя бы минимально разбирался в игровой механике онлайн-игр различного жанра, целях игроков, игровой «социологии». Представляется также необходимым ознакомление следователя со специфическим жаргоном игроков, чтобы понимать лексику допрашиваемых, специфические термины типа танк, танковать, хилл, агр, инстанс, абилка и т.д. Кроме того, в связи с тем что многие игроки находятся в других городах, а иногда и других странах, представляется необходимым активизировать вопрос дистанционных следственных действий: допроса свидетелей, потерпевших и подозреваемых, прежде всего, с использованием систем видеоконференц-связи. Отдельные разработки данного вопроса уже неоднократно предлагались различными учеными [18. С. 56; 19. С. 108–116]. Современное развитие средств электронной техники и трехмерного моделирования также допускает появление возможности производства в самое ближайшее время следственных действий с использованием различных вариантов компьютерно-опосредованной виртуальной реальности. Дистанционное производство указанных следственных действий позволит сгладить проблему расстояния и даже нахождения допрашиваемых лиц в других государствах. При допросе не стоит злоупотреблять классической рекомендацией о необходимости показать допрашиваемому общие увлечения для налаживания психологического контакта. Если у следователя, производящего допрос, реальных игровых достижений нет, такие попытки будут только смешить и раздражать допрашиваемого. А вот продемонстрировать знание специфики различных жанров игр, осведомленность о игровых новинках, знание игрового жаргона, наоборот, может иметь положительный эффект.

Следует также отметить необходимость привлечения к расследованию различных специалистов – не только программистов широкого профиля, но и специалистов – гейм-дизайнеров, которые смогут проконсультировать следователя в области игровой механики, социологии, экономики. Кроме того, разумным представляется также и приглашение психолога, поскольку зачастую у игроков, затрачивающих на участие в компьютерных играх основную часть своего дня, откладывающих дела, встречи, вкладывающих в игру существенную часть своих реальных доходов, имеются все признаки игровой зависимости.

Что касается цифрового алиби, игроки могут инсценировать себе цифровое алиби различными методами. Условно эти методы можно разделить на аппаратно-программные: 1) с использованием игровой компьютерной мыши – игрового манипулятора с возможностью программирования последовательности нажатия кнопок в специальной управляющей программемаске; 2) с использованием разрешенных игровых

автоматических ботов – внутриигровых объектов, автоматически повторяющих записанную последовательность действий; 3) с использованием запрещенных в большинстве игр внешних программ-макросов; 4) с использованием не обнаруженных разработчиком ошибок в игре «багов» или вмешательством в программный код персонажа и с использованием помощи иных лиц (знакомых, родственников, согильдийцев или лиц, зарабатывающих на «прокачке» чужих персонажей), которым предоставляется доступ к учетной записи пользователя. Изобличение инсценировки цифрового алиби возможно с учетом различных тактических рекомендаций. В первую очередь стоит запросить у администрации проекта логи игры пользователя за определенный период и привлечь специалиста из проекта. Специалисты, исследовав логи, смогут указать на алгоритмичность действий персонажа, достаточно продолжительную одинаковую последовательность, не характерную для живого игрока. Использование же помощи другого человека может отразиться недостаточным опытом в игре, не характерными действиями, неотработанным командным взаимодействием, уклонением от определенных обязательных действий, несведомленностью о каких-то игровых условиях, игровой дипломатии. Пользователь, играющий чужим персонажем, будет избегать голосового общения и уклоняться от входа в подобные программы под любыми предлогами. Данные обстоятельства могут быть

установлены при опросах или допросах в качестве свидетелей иных участников игры. Кроме того, сам подозреваемый, ссылающийся на цифровое алиби с онлайн-игрой, в ходе допроса может путаться в отдельных показаниях о своих действиях в рассматриваемое игровое время. Он может не проявить достаточной осведомленности о громких игровых событиях рассматриваемого периода, как межпользовательских (объявление мира, войны, договоренности с иными участниками), так и инициированных администрацией инвентов (от англ. event – событие), технических работах, объединении серверов и т.д.

Безусловно, в ходе расследования преступлений, совершенных в онлайн-играх, необходимо оптимально использовать рекомендации в области цифровой криминалистики, предлагаемые В.Б. Веховым, В.А. Мещеряковым, А.Н. Яковлевым, А.А. Шаевичем, С.В. Зуевым, Д.А. Степаненко и др.

Все эти рекомендации отчасти носят прогнозный характер, поскольку одним из условий необходимости разработки новой частной методики расследования является широкое распространение определенных преступлений. Для адекватной же статистики рассматриваемых преступлений необходимо понимание возможности материальной оценки «виртуального» ущерба, изменение самой парадигмы отношения к данным преступлениям как к чему-то несерьезному и не приносящему реального вреда.

ЛИТЕРАТУРА

1. Медведев А.И. Правовые отношения в пространстве виртуальных игровых миров: проблемы теории и практики // Вестник Сибирского юридического института МВД России. 2018. № 2 (31). С. 139–150.
2. Шиндин О.И. Использование онлайн-игр для подготовки и совершения коррупционных преступлений // Студенческий вестник : науч. журнал. 2021. № 1 (146), ч. 3. С. 83–85.
3. Ищенко Е.П. Криминалистика: главные направления развития // Сибирские уголовно-процессуальные и криминалистические чтения. 2012. № 1. С. 201–209.
4. Иванов В.Ю. К вопросу о классификации электронно-цифровых следов // Национальная безопасность / nota bene. 2020. № 3. С. 64–71.
5. Абрамова А.А. Значение виртуальных следов в расследовании финансирования терроризма // Общество: политика, экономика, право. 2017. № 4. С. 85–87.
6. Агibalов В.Ю. Виртуальные следы в криминалистике и уголовном процессе. М. : Юрлитинформ, 2012.
7. Толстолуцкий В.Ю. Закономерности криминалистической теории отражения, присущие субъективному этапу // Право. Вестник Нижегородского университета им. Н.И. Лобачевского. 2008. № 2. С. 203–209.
8. Лыткин Н.Н. Использование компьютерно-технических следов в расследовании преступлений против собственности : автореф. дис. ... канд. юрид. наук. М., 2007. 24 с.
9. Милашев В.А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ : автореф. дис. ... канд. юрид. наук. М., 2004. 21 с.
10. Неупокоева И.А., Шеховцова Л.С., Кочерова Л.А. Осмотр места происшествия как информационная основа расследования преступления // Закон и право. 2018. № 6. С. 136–139.
11. Семенов А.Ю. «Некоторые аспекты выявления, изъятия и исследования следов, возникающих при совершении преступлений в сфере компьютерной информации» // Сибирский юридический вестник. 2004. № 1. С. 53–55.
12. Земцова С.И., Суров О.А., Галушин П.В. Организационно-тактические аспекты производства осмотра компьютера при расследовании преступлений, связанных с незаконным оборотом «дизайнерских» наркотиков, совершаемых с использованием интернет-магазинов // Вестник Сибирского юридического института МВД России. 2016. № 3 (24). С. 18–25.
13. Поляков В.В., Слободян С.М. Анализ высокотехнологичных способов неправомерного удаленного доступа к компьютерной информации // Известия Томского политехнического университета. Инжиниринг георесурсов. 2007. Ч. 310, № 1. С. 212–216.
14. Романенко М.А. Следственный осмотр по делам о преступных нарушениях авторских прав в сфере программного обеспечения // Вестник Омского университета. Серия: Право. 2008. № 1. С. 171–175.
15. Сокол В.Ю. Растровый розыск преступников в Германии : учеб. пособие. Краснодар : Краснодар. ун-т МВД России, 2009. С. 6–37.
16. Смушкин А.Б. К вопросу об электронных следственных действиях // Законодательство. 2019. № 11. С. 76–81.
17. Еремченко В.И., Сафронкина О.В. Проблемные вопросы определения суммы материального ущерба и пути их решения при расследовании мошенничества в сфере компьютерной информации в области индустрии компьютерных игр // Общество и право. 2019. № 4 (70). С. 67.
18. Щерба С.П., Архипова Е.А. Применение видеоконференцсвязи в уголовном судопроизводстве России и зарубежных стран: опыт, проблемы, перспективы. М. : Юрлитинформ, 2016. 216 с.
19. Овчинникова О.В. Дистанционные следственные действия: современное состояние и перспективы // Юридическая наука и правоохранительная практика. 2019. № 1 (47). С. 108–116.

Статья представлена научной редакцией «Право» 26 апреля 2020 г.

Online Games as a Space for Committing Crimes

Vestnik Tomskogo gosudarstvennogo universiteta – Tomsk State University Journal, 2021, 468, 259–264.

DOI: 10.17223/15617793/468/30

Aleksandr B. Smushkin, Saratov State Law Academy (Saratov, Russian Federation). E-mail: Skif32@ya.ru

Keywords: MMORPG; incident computer space; game economy; sale of game objects; electronic object examination; investigation of crimes committed using online games.

Stating the large amount of financial resources circulating in the field of online game economy (trading in game objects, accounts, game help, etc.), the author points out that these factors cannot but cause the commission of crimes in this area. Using numerous examples, the author shows the high real value of some virtual game items and substantiates the reality of committing crimes related to the illegal seizure of these items. During the study, sociological survey and statistical methods were used. In the course of the study, about 200 players of online games of various genres were interviewed. Considering the separate functionality of some games, the author also points out the possibility of using games for the preparation, commission, and concealment of crimes. In addition, the article identifies factors that prevent law enforcement agencies from taking and investigating these crimes seriously. The author emphasizes the almost complete absence of forensic recommendations in this area. The aim of this article was to develop separate recommendations for the identification, qualification, and investigation of crimes related to online games. The author defines the types of crimes that can be committed in the area under consideration and points out certain features of their qualification. At its core, the range of crimes committed in online games, in relation to game objects or with the help of online games, is quite wide, which indicates the need to prepare a comprehensive forensic investigation methodology. Based on certain provisions of game mechanics, game economy, and game communication, the author considers certain ways of committing crimes using online games. The author also determines the features of identifying and verifying a digital alibi, using online games, to which the suspect can refer. The author defines the main investigative situations of the initial stage of the investigation and analyzes their specifics. Taking into account the specifics of the object of knowledge in the investigation of such crimes, the author suggests a new investigative action, “inspection of an electronic object”, and specifies its separate subtypes: local device examination, network examination, distributed object (files stored in cloud services and blockchains) examination, mobile device examination. The article deals with some issues of the tactics and fixation of this investigative action. In the course of the investigation, it is recommended to involve programmers of a wide profile, specifically expert game designers, who will be able to advise the investigator in the field of game mechanics, sociology, and economy. In the absence of such experts in this locality, it is possible to attract specialists from a local provider who grants access to the Internet and provides the operation of networks. The author, considering various ways of obtaining game objects, also offers various ways of monetizing them, determining their value expression in real money.

REFERENCES

1. Medvedev, A.I. (2018) Legal relationships in the space of virtual game worlds: theory and practice issues. *Vestnik Sibirskogo yuridicheskogo instituta MVD Rossii – Vestnik of Siberian Law Institute of the MIA of Russia*. 2 (31). pp. 139–150. (In Russian).
2. Shindin, O.I. (2021) Ispol'zovanie onlayn-igr dlya podgotovki i soversheniya korruptsiyonnykh prestupleniy [The use of online games for the preparation and commission of corruption crimes]. *Studencheskiy vestnik*. 1–3 (146). pp. 83–85.
3. Ishchenko, E.P. (2012) Kriminalistika: glavnye napravleniya razvitiya [Criminalistics: the main directions of development]. *Sibirskie ugovolno-protsessual'nye i kriminalisticheskie chteniya – Siberian Criminal Procedure and Criminalistic Readings*. pp. 201–209.
4. Ivanov, V.Yu. (2020) To the question on classification of digital footprint. *Natsional'naya bezopasnost' / nota bene – National Security / Nota Bene*. 3. pp. 64–71. (In Russian). DOI: 10.7256/2454-0668.2020.3.33308
5. Abramova, A.A. (2017) The value of virtual traces in the investigation of the terrorism financing. *Obshchestvo: politika, ekonomika, pravo – Society: Politics, Economics, Law*. 4. pp. 85–87. (In Russian). DOI: 10.24158/pep.2017.4.21
6. Agibalov, V.Yu. (2012) *Virtual'nye sledy v kriminalistike i ugovolnom protsesse* [Virtual Traces in Forensics and Criminal Procedure]. Moscow: Yurlitinform.
7. Tolstolutskiy, V.Yu. (2008) Regularities of the criminalistic reflection theory inherent to the subjective phase. *Vestnik Nizhegorodskogo universiteta im. N.I. Lobachevskogo – Vestnik of Lobachevsky University of Nizhni Novgorod*. 2. pp. 203–209. (In Russian).
8. Lytkin, N.N. (2007) *Ispol'zovanie komp'yuterno-tehnicheskikh sledov v rassledovanii prestupleniy protiv sobstvennosti* [The use of computer-technical traces in the investigation of crimes against property]. Abstract of Law Cand. Diss. Moscow.
9. Milashev, V.A. (2004) *Problemy taktiki poiska, fiksatsii i iz'yatiya sledov pri nepravomernom dostupe k komp'yuternoy informatsii v setyakh EVM* [Problems of tactics of search, fixation and removal of traces in case of illegal access to computer information in computer networks]. Abstract of Law Cand. Diss. Moscow.
10. Neupokoeva, I.A., Shekhovtsova, L.S. & Kocherova, L.A. (2018) Inspection of the scene as an information basis investigation of crimes. *Zakon i pravo*. 6. pp. 136–139. (In Russian). DOI: 10.24411/2073-3313-2018-10036
11. Semenov, A.Yu. (2004) Nekotorye aspekty vyavleniya, iz'yatiya i issledovaniya sledov, vznikayushchikh pri sovershenii prestupleniy v sfere komp'yuternoy informatsii [Some aspects of identification, seizure and investigation of traces arising from the commission of crimes in the field of computer information]. *Sibirskiy yuridicheskiy vestnik – Siberian Law Herald*. 1. pp. 53–55.
12. Zemtsova, S.I., Surov, O.A. & Galushin, P.V. (2016) 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. *Vestnik Sibirskogo yuridicheskogo instituta MVD Rossii – Vestnik of Siberian Law Institute of the MIA of Russia*. 3 (24). pp. 18–25. (In Russian).
13. Polyakov, V.V. & Slobodyan, S.M. (2007) Analiz vysokotekhnologichnykh sposobov nepravomernogo udalennogo dostupa k komp'yuternoy informatsii [Analysis of high-tech methods of illegal remote access to computer information]. *Izvestiya Tomskogo politekhnicheskogo universiteta. Inzhiniring georesurov – Bulletin of the Tomsk Polytechnic University. Geo Assets Engineering*. 1 (310). pp. 212–216.
14. Romanenko, M.A. (2008) Sledstvennyy osmotr po delam o prestupnykh narusheniyakh avtorskikh prav v sfere programmno obespicheniya [Investigative examination in cases of criminal copyright infringement in the field of software]. *Vestnik Omskogo universiteta. Seriya: Pravo – Herald of Omsk University. Series Law*. 1. pp. 171–175.
15. Sokol, V.Yu. (2009) *Rastrovyy rozysk prestupnikov v Germanii* [Raster Search for Criminals in Germany]. Krasnodar: Krasnodar University of the Ministry of Internal Affairs of Russia. pp. 6–37.
16. Smushkin, A.B. (2019) Electronic investigative actions. *Zakonodatel'stvo*. 11. pp. 76–81. (In Russian).

17. Eremchenko, V.I. & Safronkina, O.V. (2019) Problematic issues of determining the amount of material damage and ways to solve them in the investigation of fraud in the field of computer information in the sphere of computer games industry. *Obshchestvo i pravo – Society and Law*. 4 (70). pp. 64–68. (In Russian).
18. Shcherba, S.P. & Arkhipova, E.A. (2016) *Primenenie videokonferentsy v ugolovnom sudoproizvodstve Rossii i zarubezhnykh stran: opyt, problemy, perspektivy* [The Use of Video Conferencing in Criminal Proceedings in Russia and Foreign Countries: Experience, problems, prospects]. Moscow: Yurlitinform.
19. Ovchinnikova, O.V. (2019) Remote investigative actions: current state and prospects. *Yuridicheskaya nauka i pravookhranitel'naya praktika – Legal Science and Law Enforcement Practice*. 1 (47). pp. 108–116. (In Russian).

Received: 26 April 2020