Научная статья
УДК 343.9
EDN WWKATQ
DOI 10.17150/2411-6122.2026.2.37-44

Тактические особенности производства отдельных следственных действий при расследовании мошенничества в сфере компьютерной информации

В.В. Коломинов

Байкальский государственный университет, г. Иркутск, Российская Федерация, KolominovVV@bgu.ru

Аннотация. Анализируются особенности проведения следственных действий при расследовании мошенничества в сфере компьютерной информации. Подчеркивается, что для достижения высоких результатов такие действия требуют тщательного предварительного планирования. При подготовке к следственным мероприятиям по подобным преступлениям целесообразно рассматривать возможность привлечения специалистов — это может повысить их эффективность. Делается вывод, что проведение отдельных следственных действий в расследовании мошенничества в сфере компьютерной информации является одним из средств сбора электронной доказательной информации, а также установления виновных лиц, совершивших указанное преступление. Использование результатов следственных действий позволяет осуществить проверку выдвинутых версий и понять, какие тактические приемы необходимо применять для дальнейшего проведения расследований мошенничества в сфере компьютерной информации.

Ключевые слова: расследование, мошенничество, информация, тактика, осмотр, обыск.

Для цитирования: Коломинов В.В. Тактические особенности производства отдельных следственных действий при расследовании мошенничества в сфере компьютерной информации / В.В. Коломинов. — DOI 10.17150/2411-6122.2026.2.37-44. — EDN WWKATQ // Сибирские уголовно-процессуальные и криминалистические чтения. — 2026. — № 2. — С. 37–44.

Original article

Tactical Features of Some Investigative Actions in the Investigation of Computer Fraud

V.V. Kolominov

Baikal State University, Irkutsk, the Russian Federation, KolominovVV@bgu.ru

Abstract. Specific features of investigative actions used in the investigation of computer fraud are analyzed. It is stressed that such actions require a thorough preliminary planning in order to achieve good results. When preparing the investigative activities for such crimes it is advisable to consider the possibility of involving experts, as it could increase the effectiveness of the activities. It is concluded that carrying out certain investigative actions in the investigation of computer fraud is one of the ways of collecting electronic information proof, and establishing the guilty persons who committed the crime. Results obtained through investigative actions make it possible to verify previously proposed leads and understand which tactical methods should be used for the future investigation of computer frauds.

 DOI 10.17150/2411-6122.2026.2.37-44 ISSN 2411-6122

Keywords: investigation, fraud, information, tactics, inspection, search.
For citation: Kolominov V.V. Tactical Features of Some Investigative Actions in the Investigation of Computer Fraud. *Sibirskie Ugolovno-Processual'nye i Kriminalisticheskie Chteniya = Siberian Criminal Procedure and Criminalistic Readings*, 2026, no 2, pp. 37–44. (In Russian). EDN: WWKATQ. DOI: 10.17150/2411-6122.2026.2.37-44.

Результативное проведение расследования мошенничества в сфере компьютерной информации, прежде всего, связано с эффективным проведением отдельных следственных действий, направленных на проверку следственных версий путем сбора (получения) доказательств в предусмотренном уголовным процессуальным законодательством порядке, а также проверку уже полученных доказательств.

Каждое следственное действие имеет не только четко определенные процессуальные, но и тактические особенности его проведения.

По мнению В.Р. Гайнельзянова, тактические особенности — это рекомендация о возможных альтернативных вариантах проведения процессуальных действий или принятия тактических решений. Еще до начала непосредственного проведения следственных действий следователю необходимо решить определенные вопросы, касающихся времени и места, состава участников, подготовке доказательств и определении очередности их предъявления, средств фиксации и полученных результатов и т.д. [1].

Одним из первых следственных действий, предоставляющим возможность быстро зафиксировать следы противоправных деяний во время расследования преступления указанной категории, является проведение осмотра.

Осмотр компьютерных данных проводит следователь путем отображения в протоколе обзора информации, которую они содержат, в форме, подходящей для восприятия их содержания (с помощью фотосъемки, видеозаписи, съемки и/или видеозаписи экрана и т.п., или в бумажной форме) [2].

Рассмотрим некоторые тактические особенности, возникающие в ходе осмотра.

По утверждению В.И. Алескерова [3], осмотр места происшествия в расследовании мошенничества в сфере компьютерной информации, способствует выяснению ряда важных вопросов: на каком объекте (на каком конкретно компьютере, в каком структурном подразделении учреждения) произошло событие; каково во время осмотра состояние средств защиты информации, охраны помещений, оборудование и ряд других вопросов.

Разделяя такой подход, предлагаем дополнить этот перечень вопросами, которые нуждаются в выяснении в процессе осмотра: где могут храниться следы совершения таких противоправных деяний и их локализация; характер причиненного вреда; место, время и обстоятельства совершения преступления и др.

В то же время заметим, что перечень вопросов не может быть исчерпывающим. Его следует уточнять в зависимости от цели проведения осмотра и обстановки совершения правонарушения.

В несложных случаях, когда речь идет об одном компьютерном средстве, которое находится у лица, можно ограничиться привлечением одного специалиста.

В сложных случаях, когда имеются объединенная компьютерная сеть, значительное количество средств инфор-

мационных — компьютерных технологий и т.п., целесообразно привлекать к проведению осмотра места происшествия нескольких специалистов в отрасли информационных компьютерных технологий.

С.В. Зуев считает, что применение программных средств проведения осмотра, должно соответствовать двум основным критериям:

1) быть с открытой лицензией или находиться на балансе правоохранительных органов, чтобы можно было проверить корректность их работы;

2) в случае использования открытого программного обеспечения необходимо соответствующую копию с хеш-суммой диска приобщить как приложение к протоколу [4].

По нашему убеждению, необходимо постоянно следить за созданием и использованием современных программных средств в международной практике, касательно расследования указанных противоправных деяний. Прежде всего, это поможет следователю ориентироваться в самых эффективных современных программных средствах, а также применять их во время проведения осмотра места происшествия и других следственных действиях.

По прибытии на место происшествия возникает необходимость решить ряд организационных и технических вопросов:

1) обеспечение целостности и охраны места проведения осмотра; 2) определение, что будет объектами осмотра, их количество, специфика и последовательность проведения; 3) подготовка соответствующего оборудования; 4) выяснение у лиц информации, которой они располагают по поводу произошедшего.

Если следователь сочтет целесообразным, понятые могут быть приглашены для участия в проведении осмотра (ст. 60 УПК РФ).

Верным является предложение Е.П. Ищенко приглашать понятыми к осмотру в уголовных правонарушениях указанной категории лиц, осведомленных о работе информационных компьютерных технологий [5]. Это будет служить не только объективности содержания проведения осмотра, но и правильному отражению обстоятельств и фактов, их надлежащему фиксированию в протоколе осмотра, что будет иметь важное доказательное значение в уголовном производстве.

В то же время каждое действие следователя должно быть разъяснено понятым лицам, в частности должно быть разъяснено его содержание, сущность и цель, а также в случае получения вопросов от понятых — даны ответы, что обязательно отмечают в протоколе.

Процесс рабочего этапа проведения осмотра места происшествия предусматривает две стадии: статическую и динамическую.

В процессе осмотра места происшествия на статической стадии необходимо соблюдать следующие рекомендации [6]:

1) сфотографировать средство (средства) информационных компьютерных технологий, чтобы зафиксировать его (их) состояние;

2) прислушаться и присмотреться к системе, чтобы определить, работает ли средство информационно-компьютерных технологий;

3) прежде всего, осуществить осмотр средств, которые находятся во включенном состоянии, детально их описать и сфотографировать;

4) использовать в протоколе компьютерную терминологию.

Когда полностью осуществлен статический осмотр места происшествия,

 DOI 10.17150/2411-6122.2026.2.37-44 ISSN 2411-6122

следует переходить к следующей стадии — динамической, заключающейся во всестороннем обзоре отдельных предметов, в случае необходимости сдвигая их с места.

В мошенничестве в сфере компьютерной информации, по нашему мнению, динамическая стадия связана с непосредственным обследованием информации, которая находится в средстве (средствах) информационных компьютерных технологий.

В случае установки пароля на средстве информационно-компьютерных технологий по возможности следует выяснить пароль пользователя, а также установить, включено ли шифрование диска. В случае, когда пароль доступа установить невозможно, необходимо поручить специалисту изготовить дамп (копию) оперативной памяти с целью отыскания хранящихся в ней паролей до момента выключения [7].

Если есть необходимость изъять определенные аппаратные (технические) устройства, нужно следовать таким рекомендациям [8]:

– перед отсоединением от питания компьютерной техники необходимо завершить выполнение всех программ, работающих на средстве информационно-компьютерных технологий, поскольку некорректный выход из них может привести к потере доказательной информации или порчи программного обеспечения, что делает невозможным дальнейшее проведение экспертизы;

– промаркировать оборудование перед отключением и удалением;

– опломбировать корпус аппаратного средства, чтобы сделать невозможным его раскрытие;

– упаковать изъятые устройства.

В случае запрета временного изъятия, необходимо с помощью соответствующих средств изготовить копии информации. Копирование такой информации осуществляют с привлечением специалиста [9].

Технически есть три способа получения копий электронных носителей, содержащих следы совершения рассматриваемого противоправного деяния:

1) создание образа соответствующего носителя;

2) создание дубликата носителя;

3) логическое копирование отдельных данных.

В первом случае с помощью программных средств создают соответствующий образ носителя, хранящийся как файл на другом диске.

Во втором случае осуществляют копирование данных один в один, в результате чего получают точную копию носителя. Такой носитель можно безопасно хранить не опасаясь, что данные могут быть испорчены.

В третьем случае осуществляют копирование отдельных файлов, вследствие чего получают копии, но не структуру носителя. Однако, если на носителе находится скрытая информация, то она не будет скопирована.

Каждый из указанных случаев следует применять в зависимости от конкретной ситуации по рекомендации специалиста.

Заключительный этап осмотра предусматривает:

1) составление протокола осмотра места происшествия;

2) упаковку изъятых объектов, и принятие мер по их сохранению;

3) принятие мер по заявлениям, поступившим от участников осмотра места происшествия.

Протокол осмотра места происшествия должен соответствовать требованиям, предусмотренным в ст. 180 УПК РФ, и иметь три части: 1) вводную; 2) описательную; 3) заключительную.

Водная часть не имеет каких-либо особенностей.

Составление описательной части протокола осмотра в преступлениях в расследовании мошенничества в сфере компьютерной информации, имеет определенную специфику, очерченную терминологией и особенностями описания средств информационно-компьютерных технологий. Поэтому при составлении протокола, по нашему мнению, следует придерживаться следующих тактических рекомендаций:

– каждое изучаемое средство информационных компьютерных технологий должен быть четко описан в протоколе (марка, модель, заводской и инвентарный номера, технические особенности, его местоположение и т.д.);

– если происходило исследование программных средств, необходимо отметить, как они были исследованы и в каком именно средстве информационно-компьютерных технологий;

– отдельно указывать время исследования каждого средства информационных компьютерных технологий;

– важна правильная запись всех серийных номеров, хэш-сумм, названий устройств и т.д.;

– в случае использования определенных программ для исследования средств информационных компьютерных технологий необходимо сделать отметку об этом;

– особую ценность для расследования будут иметь лог-файлы (Log file), т.е. файлы в которых содержится информация о работе средства информационных компьютерных технологий.

Целесообразно все изъятое при осмотре места происшествия указывать в заключительной части протокола, перечислив по списку. Это облегчит в дальнейшем учет изъятого [10].

Необходимо помнить, что при изготовлении оригинала документа в электронной форме после завершения осмотра места происшествия специалист по поручению следователя в произвольной форме составляет письменное объяснение, которое вместе с отображением записи процессуального действия присоединяют как приложения к протоколу осмотра места происшествия [11].

В случае временного изъятия информационных систем, которые являются доказательствами преступления, необходимо принять меры по их сохранению. В таком случае следует действовать в соответствии со ст. 183 УПК РФ. Следователь по согласованию с прокурором не позднее следующего дня после изъятия имущества должны обратиться в суд с ходатайством об аресте имущества с целью сохранения вещественных доказательств, проведение экспертного исследования или преодоления системы логической защиты. Устойчивой является практика, что перед обращением с соответствующим ходатайством к судье, временно изъятое имущество постановлением следователя, приобщают к уголовному производству как вещественное доказательство, а постановление приобщают как приложение к ходатайству. Важно, что постановлением следователя как вещественное доказательство к уголовному производству также приобщают средства информационных компьютерных технологий, изъятые на основании постановления суда о проведении осмотра. Вынесению постановления предшествует проведение детального осмотра изъятого имущества, если во время проведения осмотра места происшествия это не сделали.

Еще одним эффективным следственным действием расследования мошенничества в сфере компьютерной информации является обыск.

 DOI 10.17150/2411-6122.2026.2.37-44 ISSN 2411-6122

Обыск является одним из распространенных следственных действий, которые следователи используют для обнаружения, фиксации и изъятия доказательной информации, имеющей значение для выяснения обстоятельств совершения преступления, установления лиц, его совершивших.

В то же время обыску присущи определенные процессуальные и тактические особенности, в частности целью обыска является более конкретной и предусматривает также отыскание средств или орудий преступления.

Проведение обыска имеет принудительный характер и четко определенные процессуальные особенности.

Учитывая это, рассмотрим специфику проведения обыска в расследовании мошенничества в сфере компьютерной информации.

Исследовав имеющиеся в отечественной криминалистической литературе определения обыска, можно сделать вывод, что они существенно не разнятся.

В свое время по поводу проведения обыска С.Н. Миронов замечал, что кто будет ограничиваться обыском ящиков и сундуков, кроватей, дымоходов, тот вряд ли что-нибудь найдет [12].

В практической деятельности неотложность проведения обыска обосновывают в постановлении, на основании которого и проводят обыск.

Среди тактических особенностей проведения обыска в расследовании мошенничества в сфере компьютерной информации, можно выделить следующие:

1) соблюдение принципа внезапности при прибытии и вхождении в помещение, в котором будет проведен обыск;

2) запрет использования для поиска тайников с магнитными носителями;

3) необходимость быстрой проработки значительного объема выявленной информации с целью установления ее ценности для расследования;

4) проведение обыска только на одном или нескольких средствах информационно-компьютерных технологий, принадлежащих к локальной сети [6].

На наш взгляд, дополнить этот перечень можно такими тактическими и процессуальными особенностями:

– в ходатайстве об обыске следует четко определить средства информационно-компьютерных технологий, которые необходимо отыскать, а до проведения обыска ознакомиться с их характеристикой;

– при обыске обнаружить доступ или возможность доступа к средствам информационных компьютерных технологий;

– установить психологический контакта с лицом, у которого проводят обыск;

– направить внимание на все устройства хранения данных (флешки, диски и т.д.).

Заметим, что этот перечень не является исчерпывающим и может быть дополнен в зависимости от соответствующей следственной ситуации и других обстоятельств. В большинстве случаев во время проведения обыска применяют такие тактические особенности, как и во время проведения осмотра.

Поэтому с целью обеспечения результативности проведения обыска в расследовании мошенничества в сфере компьютерной информации, необходимо тщательно его планировать заранее.

Можно сделать вывод, что знание тактических особенностей производства следственных действий при расследовании компьютерных мошенничеств необходимо для эффективного поиска, фиксации и изъятия цифровых доказательств. Эти знания помогают оперативно закрепить информацию, преодолеть противодействие расследованию и привлечь профильных специалистов.

Список использованной литературы

1. Гайнельзянова В.Р. Возможности судебной компьютерно-технической экспертизы при расследовании преступлений в сфере компьютерной информации / В.Р. Гайнельзянова. — EDN LMFXEE // Вестник Уфимского юридического института МВД России. — 2021. — № 1. — С. 144–149.

2. Лантух Э.В. Использование специальных знаний при расследовании преступлений в сфере компьютерной информации / Э.В. Лантух, В.С. Ишигеев, О.П. Грибунов. — DOI 10.17150/2500-4255.2020.14(6).882-890. — EDN VHTUKP // Всероссийский криминологический журнал. — 2020. — Т. 14, № 6. — С. 882–890.

3. Алескеров В.И. Раскрытие преступлений в сфере телекоммуникаций и компьютерной информации : учеб.-практ. пособие / В.И. Алескеров, О.Н. Колокольчикова. — Домодедово, 2016. — 118 с.

4. Зуев С.В. Осмотр и изъятие электронных носителей информации при проведении следственных действий и оперативно-розыскных мероприятий / С.В. Зуев. — EDN UNYMRO // Законность. — 2018. — № 4. — С. 58–60.

5. Ищенко Е.П. Виртуальное пространство как объект криминалистического познания / Е.П. Ищенко. — EDN SINXZR // Криминалистика и судебно-экспертная деятельность в условиях современности : материалы Междунар. науч.-практ. конф., Краснодар, 26 апр. 2013 г. : в 2 т. — Краснодар, 2013. — Т. 1. — С. 16–23.

6. Коломинов В.В. Установление места совершения преступления в процессе расследования мошенничества в сфере компьютерной информации / В.В. Коломинов. — EDN VCYXOZ // Криминалистические чтения на Байкале — 2015 : материалы Междунар. науч.-практ. конф., Иркутск, 18–19 июня 2015 г. / отв. ред. Д.А. Степаненко. — Иркутск, 2015. — С. 264–268.

7. Бердникова О.П. Особенности расследования мошенничества в сфере компьютерной информации : учеб. пособие / О.П. Бердникова, Р.А. Дерюгин. — Екатеринбург : Изд-во Урал. юрид. ин-та МВД России, 2021. — 83 с.

8. Шигуров А.В. Проблемы правового регулирования изъятия электронных носителей информации и копирования с них информации при производстве следственных действий / А.В. Шигуров, Н.А. Подольный. — DOI 10.36511/2078-5356-2020-1-169-174. — EDN CHWOBT // Юридическая наука и практика: Вестник Нижегородской академии МВД России. — 2020. — № 1. — С. 169–174.

9. Комаров И.М. Правовые и криминалистические проблемы расследования мошенничества в сфере компьютерной информации / И.М. Комаров. — EDN VRODFJ // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. — 2015. — № 1. — С. 12–15.

10. Васюков В.Ф. Тактические проблемы проведения осмотра места происшествия при расследовании мошенничества в сфере компьютерной информации / В.Ф. Васюков. — EDN XRJUGT // Право и образование. — 2017. — № 2. — С. 103–110.

11. Харина Е.А. К вопросу о криминалистической характеристике мошенничества в сфере компьютерной информации / Е.А. Харина. — DOI 10.18572/1812-3783-2023-11-11-15. — EDN XVAGVR // Российский следователь. — 2023. — № 11. — С. 11–15.

12. Выявление, пресечение и документирование преступлений, связанных с мошенничеством в сфере компьютерной информации, предусмотренных статьей 159.6 Уголовного кодекса Российской Федерации : метод. рекомендации / сост. С.Н. Миронов [и др.]. — Казань : Изд-во КЮИ МВД России, 2017. — 51 с.

References

1. Gainelzyanova V.R. Possibilities of Forensic Computer-Technical Expertise in the Investigation of Crimes in the Field of Computer Information. *Vestnik Ufimskogo yuridicheskogo instituta MVD Rossii = Bulletin of Ufa Law Institute of MIA of Russia*, 2021, no. 1, pp. 144–149. (In Russian). EDN: LMFXEE.

2. Lantukh E.V., Ishigeev V.S., Gribunov O.P. The Use of Special Knowledge in the Investigation of Computer Crimes. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Crim-*

inology, 2020, vol. 14, no. 6, pp. 882–890. (In Russian). EDN: VHTUKP. DOI: 10.17150/2500-4255.2020.14(6).882-890.

3. Aleskerov V.I. *Solving Crimes in the Sphere of Telecommunications and Computer Information.* Domodedovo, 2016. 118 p.

4. Zuyev S.V. Search for and Seizure of Electronic Information Devices in the Course of Investigative Actions and Operative and Search Activities. *Zakonnost' = Legality*, 2018, no. 4, pp. 58–60. (In Russian). EDN: UNYMRO.

5. Ishhenko, E.P. Virtual Space as an Object of Forensic Cognition. In *Criminalistics and Forensic Work in Modern Conditions.* Materials of the International Scientific and Practical Conference, Krasnodar, April 26, 2013. Krasnodar, 2013. Vol. 1, pp. 16–23. (In Russian). EDN: SINXZR.

6. Kolominov V.V. Establishing the Location of the Crime Scene in the Investigation of Computer Frauds. In Stepanenko D.A. (ed.). *Criminalistic Readings on Lake Baikal — 2015. Proceedings of the International Scientific and Practical Conference, Irkutsk, June 18–19, 2015.* Irkutsk, 2015, pp. 264–268. (In Russian). EDN: VCYXOZ.

7. Berdnikova O.P., Deryugin R.A. *Specific Features of Investigating Computer Frauds.* Ekaterinburg, Ural Law Institute of the Ministry of Internal Affairs of the Russian Federation Publ., 2021. 83 p.

8. Shigurov A.V, Podolnyy N.A. Problems of Legal Regulation of the Seizure of Electronic Information Carriers and Copying Information from them in the Course of Investigative Actions. *Yuridicheskaya nauka i praktika: Vestnik Nizhegorodskoi akademii MVD Rossii = Legal Science and Practical: Journal of Nizhniy Novgorod Academy of the Ministry of the Interior of the Russian Federation*, 2020, no. 1, pp. 169–174. (In Russian). EDN: CHWOBT. DOI: 10.36511/2078-5356-2020-1-169-174.

9. Komarov I.M. Legal and Forensic Issues of Fraud Investigation in the Sphere of Computer Information. *Prestupnost' v sfere informatsionnykh i telekommunikatsionnykh tekhnologii: problemy preduprezhdeniya, raskrytiya i rassledovaniya prestuplenii = Crime in the Sphere of Information and Telecommunication Technologies: Problems of Prevention, Detection and Investigation of Crimes*, 2015, no. 1, pp. 12–15. (In Russian). EDN: VRODFJ.

10. Vasyukov V.F. Tactical Problems of Conducting a Scene Examination in the Investigation of Fraud in the Sphere of Computer Information. *Pravo i obrazovanie = Law and Education*, 2017, no. 2, pp. 103–110. (In Russian). EDN: XRJUGT.

11. Kharina E.A. On the Criminalistic Characteristics of Cyber Fraud. *Rossiiskii sledovatel' = Russian Investigator*, 2023, no. 11, pp. 11–15. (In Russian). EDN: XVAGVR. DOI: 10.18572/1812-3783-2023-11-11-15.

12. Mironov S.N. [et al] (eds). *Detection, Suppression and Registration of Crimes Connected with Computer Fraud under Art. 159.6 of the Criminal Code of the Russian Federation*. Kazan Law Institute of the Ministry of Internal Affairs of Russia Publ., 2017. 51 p.

Информация об авторе

Коломинов Вячеслав Валентинович — кандидат юридических наук, доцент, доцент кафедры криминалистики, судебных экспертиз и юридической психологии, Институт юстиции, Байкальский государственный университет, 664003, Российская Федерация, г. Иркутск, ул. Ленина, 11, https:// orcid.org/0000-0001-9797-0908, SPIN-код: 4690-0019.

Author Information

Kolominov, Vyacheslav V. — Ph.D. in Law, Ass. Professor, Department of Criminalistics, Forensic Examination and Legal Psychology, Institute of Justice, Baikal State University, 11 Lenin Str., Irkutsk, 664003, the Russian Federation, https://orcid.org/0000-0001-9797-0908, SPIN-Code: 4690-0019.

Поступила в редакцию / Received 07.05.26

Одобрена после рецензирования / Approved after reviewing 08.06.26

Принята к публикации / Accepted 18.06.26

Дата онлайн-размещения / Available online 30.06.26