УДК 343.9

ТАКТИКО-КРИМИНАЛИСТИЧЕСКИЕ И ПРОЦЕССУАЛЬНЫЕ ОСОБЕННОСТИ ПРОВЕДЕНИЯ ОСМОТРА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

А. Н. Примаков
кандидат юридических наук,
доцент кафедры уголовного права, уголовного процесса и криминалистики
Могилевского института МВД (Беларусь)

Д. В. Романюк
курсант факультета милиции
Могилевского института МВД (Беларусь)

На основе результатов анализа норм уголовно-процессуального законодательства Республики Беларусь и Российской Федерации, практики их применения в судебно-следственной деятельности в статье излагаются как тактико-криминалистические, так и процессуальные особенности проведения осмотра компьютерной информации при раскрытии и расследовании преступлений.

Для повышения эффективности производства осмотра компьютерной информации предлагается внести в действующий уголовно-процессуальный закон Республики Беларусь изменения, направленные на дополнительную регламентацию положений, связанных с порядком проведения данного следственного действия в жилище или ином законном владении. Определено, что организация и тактика указанного вида осмотра, его результативность зависят, прежде всего, от характеристики компьютерной информации и применяемых для ее охраны средств защиты, а также имеющегося в арсенале следственных органов технического оснащения, необходимого для ее обнаружения, фиксации и изъятия.

Ключевые слова: *уголовно-процессуальная деятельность, расследование, следственный осмотр, тактика, компьютерная информация, информационно-телекоммуникационные технологии, компьютерные следы.*

Одним из наиболее распространенных и неотложных следственных действий, результаты которого выступают информационной основой для раскрытия и последующего успешного расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий и сети Интернет, является осмотр компьютерной информации [1, с. 189]. В Уголовно-процессуальном кодексе Республики Беларусь (далее — УПК), наряду с осмотром места происшествия и другими видами следственного осмотра, осмотр компьютерной информации обозначен в отдельной норме как самостоятельное следственное действие. Прежде всего, это обусловлено его спецификой — наличием виртуального компонента, то есть объекта или состояния, одномоментно включающего материальные (физические объекты, устройства) и нематериальные (представляемые мыслительные образы) свойства, доступ к которому осуществляется определенным, как правило, электронно-цифровым способом.

Основанием для проведения осмотра компьютерной информации является наличие достаточных данных полагать, что в ходе следственного действия будут или могут быть обнаружены следы преступления и иные материальные объекты, выяснены другие обстоятельства, имеющие значение для уголовного дела (ст. 203 УПК). Процессуальный порядок и условия его производства закреплены в ч. 3^1 ст. 204 и ст. 204^1 УПК, в которых определены место, где должно проводиться данное следственное действие, возможность осуществления уполномоченными лицами, помимо предусмотренных в общем порядке, действий, связанных с функционалом осматриваемых информационных систем и их ресурсов, а также использованием научно-

технических средств; установлены процессуальные требования по документальному оформлению осмотра, право на копирование и изъятие полученной в рамках его проведения информации [2].

Однако, как представляется, такое редакционное изложение указанных норм не в полной мере позволяет ясно выразить некоторые понятийные категории рассматриваемого следственного действия, прежде всего, связанные с определением и содержанием компьютерной информации, компьютерных источников и электронных носителей информации, фиксацией и изъятием их цифровых следов, использованием некоторых форм специальных знаний, что зачастую на практике порождает ряд проблем и процессуальных ошибок. Предложения по их разрешению нами излагались в ранее опубликованной работе [3, с. 110–111].

Организация и тактика проведения осмотра компьютерной информации в первую очередь зависят от ее вида (числовая, текстовая, графическая, звуковая и т. д.) и применяемых для ее охраны средств защиты. Доступ к компьютерной информации ограниченного распространения (об индикационных данных, о частной жизни лица, о личной и семейной тайне и др.) либо к информации, защищаемой процедурой аутентификации, согласно ч. 2 ст. 204[1] УПК, осуществляется двумя альтернативными способами:

1) путем получения согласия пользователя (обладателя) компьютерной информации на проведение ее осмотра с обязательным непосредственным его участием и предоставлением сведений, необходимых для прохождения процедуры аутентификации;

2) без получения согласия пользователя (обладателя) компьютерной информации на проведение ее осмотра по постановлению следователя (лица, производящего дознание), санкционированного прокурором как с предоставлением сведений, необходимых для прохождения процедуры аутентификации, так и без таковых.

При этом в ч. 2 ст. 204[1] УПК прямо не указано, должен ли обязательно при проведении данного следственного действия присутствовать, как в первом случае, пользователь (обладатель) компьютерной информации. Представляется, что в таком случае его присутствие не обязательно, однако как же в такой ситуации можно осмотреть компьютерную информацию, доступ к которой осуществляется посредством аутентификации, если не имеется исходных сведений о логине и пароле пользователя либо последний отказывается их предоставлять. Следовательно, при таких обстоятельствах производство осмотра самостоятельно следователем (лицом, производящим дознание) невозможно, за исключением случаев, когда требуемые данные получены оперативным путем либо в результате проведения других следственных действий (осмотра места происшествия, обыска, выемки и др.).

Альтернативными способами решения данной задачи в рассматриваемой ситуации также являются:

− направление в порядке ст. 184 УПК поручения о проведении осмотра компьютерной информации сотрудникам криминалистических отделов областных управлений и центрального аппарата Следственного комитета Республики Беларусь, которые при исполнении поручения смогут применить для извлечения необходимой доказательственной информации наиболее широкий арсенал аппаратных комплексов, технических средств и специализированных программ («Мобильный криминалист», UFED);

− исследование компьютерной информации в рамках проведения судебной компьютерно-технической экспертизы или судебной экспертизы радиоэлектронных устройств и электробытовых приборов; при назначении этих видов экспертных исследований по техническим средствам, изъятие которых производилось при проведении других следственных действий без санкции прокурора, последующий их осмотр следует осуществлять с учетом требований ст. 204[1] УПК.

Очень важно перед началом осмотра компьютерной информации составить план его проведения с обязательным отражением криминалистических устройств и

инструментов, применение которых может повысить результативность данного следственного действия. Следователю (лицу, производящему дознание) следует определить, какая конкретно компьютерная информация, свидетельствующая о признаках совершенного преступления, может быть обнаружена на обследуемом электронном носителе, после чего посредством проверки следственных версий о механизме взаимодействия технических средств и электронных элементов попытаться установить материальные и компьютерные следы преступления.

Необходимо определить конкретную цель и задачи следственного действия, основные области (места) поиска компьютерной информации, имеющей доказательственное значение, с учетом предъявляемых процессуальных требований сформировать тактический замысел проведения осмотра, что зачастую предопределяется фактическим характером и обстоятельствами преступного посягательства, мотивом и целью лица, его совершившего.

Общей целью проведения осмотра компьютерной информации является получение входящих в предмет доказывания по уголовному делу сведений об обстоятельствах совершенного преступления либо иных данных, имеющих, как правило, розыскное значение. Для ее достижения следователю (лицу, производящему дознание) следует изучить состояние и свойства компьютерной информации, наличие или отсутствие внесенных в ее содержание изменений, установить причинно-следственные связи и последовательность совершаемых преступных действий, выявить и изъять данные, которые имеют доказательственное значение для уголовного дела и его уголовно-правовой квалификации.

С точки зрения материально-технического оснащения и возможности использования специальных знаний осмотр компьютерной информации наиболее целесообразно проводить по месту нахождения органа, осуществляющего уголовное преследование. При необходимости данное следственное действие может быть проведено и по месту нахождения объекта осмотра или лица, обладающего компьютерной информацией. При этом не совсем ясной представляется позиция законодателя в части проведения указанного вида осмотра в жилище, поскольку в ст. 204[1] УПК, непосредственно регламентирующей порядок проведения следственного действия, об этом ничего не указано. По общему правилу, в соответствии со ст. 204 УПК, к проведению осмотра жилища, в том числе объектов, находящихся в нем, предъявляются определенные процессуальные требования (наличие не менее двух понятых и постоянно проживающего совершеннолетнего лица). Однако возникает вопрос, следует ли учитывать эти требования при проведении осмотра компьютерной информации, проводимого в жилище.

По нашему мнению, в таком случае необходимо руководствоваться положениями ст. 204 УПК, не делая в отношении данного вида осмотра исключения, поскольку фактически следственное действие производится в жилище, нарушает право на его неприкосновенность, а значит, на порядок его проведения должны распространяться предусмотренные указанной нормой требования.

Об этом свидетельствует и законодательная конструкция нормы, регламентирующей другое следственное действие, не являющееся при этом отдельным видом следственного осмотра, выемки, проведение которой в жилище против воли собственника осуществляется в соответствии с ч. 7 ст. 204 УПК, то есть по правилам проведения осмотра жилища с соблюдением необходимых уголовно-процессуальных требований (ч. 2 ст. 210 УПК).

Непосредственно на рабочем этапе при проведении осмотра компьютерной информации тактически грамотно разделить его проведение на виды в зависимости от процессуального статуса обладателя информации (потерпевший, подозреваемый, обвиняемый).

При осмотре компьютерной информации, принадлежащей потерпевшему, не требуется производить ее исследование в полном объеме, поскольку, как правило,

пределы содержания такой информации ограничены ее видом и обстоятельствами совершенного преступления. Таким образом, следует установить следующую информацию: объем и содержание компьютерной информации, которая использовалась для совершения преступного деяния; способ предоставления к ней доступа, оставленные при этом материальные (цифровые) следы (журналы и отчеты операционной системы, иных приложений и программ, лог-файлы, электронные документы, файлы программного обеспечения); компьютерные программы и приложения, посредством которых осуществлялся контакт (переписка, отправка сообщений) потерпевшего с подозреваемым; иные обстоятельства, которые могут иметь значение для расследования преступления.

При осмотре компьютерной информации, принадлежащей подозреваемому или обвиняемому, помимо большого объема данных о причастности к совершенному преступлению, которые следует обнаружить и зафиксировать, необходимо отразить сведения, характеризующие личность подозреваемого (например, интерес к компьютерным технологиям, их возможностям для совершения преступлений, наличие посещаемых интернет-ресурсов и др.), а также иные сведения, которые могут содержать следы других, в том числе латентных или нераскрытых, преступлений.

Исходя из изложенного, следует попытаться установить следующую информацию: о факте преступного посягательства, действиях по его подготовке и сокрытию, оставленных при этом компьютерных (цифровых) следах; о содержании и результатах использования полученных в рамках неправомерного доступа данных в преступных и иных целях; о компьютерных программах и средствах, используемых для разработки вредоносных программ и непосредственно для совершения преступлений; о жертвах преступлений, (например, список IP-адресов компьютеров, к которым осуществлялся несанкционированный доступ, список номеров банковских платежных карт, используемых для совершения хищений денежных средств и др.); о регистрации подозреваемым (обвиняемым) в сети Интернет, в различных мессенджерах и социальных сетях фейковых аккаунтов (учетных записей пользователя) и содержании имеющихся в них электронных переписок (отправленных сообщений).

Анализ материалов следственно-судебной практики расследования киберпреступлений показывает, что к наиболее типичным местам проверки наличия либо отсутствия хранения криминалистически значимой компьютерной информации на жестких магнитных дисках компьютерного устройства подозреваемого (обвиняемого) следует отнести директории, связанные прежде всего с установкой программного обеспечения (для определения используемых на компьютере программ), с хранением временных копий файлов (для осмотра файлов, которые последние открывались на компьютере), личных документов, ярлыков программ и файлов, расположенных на рабочем столе компьютера, а также удаленных или перемещенных в корзину либо загруженных из сети Интернет файлов.

Фиксировать проведение осмотра компьютерной информации по возможности следует посредством осуществления видеозаписи экрана компьютерного или мобильного устройства, посредством установки видеокамеры, направленной на экран осматриваемого объекта, с последующим осуществлением копирования соответствующего видеофайла на электронный носитель. Такой подход обеспечивает наиболее полное отражение порядка осмотра и минимизирует утрату информации, имеющей доказательственное значение.

Таким образом, в заключение можно сделать вывод о том, что организация и тактика проведения осмотра компьютерной информации зависит прежде всего от ее вида и применяемых для ее охраны средств защиты. Непосредственно при проведении осмотра тактически рационально разделить его, учитывая при этом не только традиционные этапы проведения следственного действия (подготовительный, рабочий и заключительный), но еще и виды информации в зависимости от процессуального статуса ее обладателя (потерпевший, подозреваемый, обвиняемый).

Для получения наибольшей результативности осмотра и исследования компьютерной информации, особенно в случаях, требующих для установления доступа к объекту осмотра обязательного ввода аутентификационных данных, необходимо применять специализированные аппаратные комплексы, технические средства и программы, состоящие на вооружении в криминалистических и экспертных подразделениях Республики Беларусь.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Казачек, Е. Ю. О некоторых особенностях осмотра трупа, обнаруженного на месте происшествия с признаками изнасилования / Е. Ю. Казачек // Расследование преступлений: проблемы и пути их решения : сб. науч.-практ. тр. — Вып. 4. — М., 2014. — С. 187–191.

2. Уголовно-процессуальный кодекс Республики Беларусь : 16 июля 1999 г. № 295-З : принят Палатой представителей 24 июня 1999 г. : одобр. Советом Респ. 30 июня 1999 г. : в ред. Закона Респ. Беларусь от 8 янв. 2024 г. // ЭТАЛОН : информ.-поисковая система (дата обращения: 15.10.2024).

3. Примаков, А. Н. Об особенностях правового регулирования осмотра компьютерной информации / А. Н. Примаков, С. Г. Полевиков // Актуальные проблемы уголовного процесса и криминалистики : сб. науч. ст. / М-во внутр. дел Респ. Беларусь, учреждение образования «Могилевский институт Министерства внутренних дел Республики Беларусь» ; редкол.: Ю. П. Шкаплеров (пред.) [и др.]. — Могилев : Могилев. ин-т МВД, 2023. — 1 CD-ROM.

Поступила в редакцию 01.11.2024 г.

Primakov A. N., Romanyuk D. V.

TACTICAL, FORENSIC AND PROCEDURAL FEATURES OF COMPUTER INFORMATION INSPECTION

Based on the results of the analysis of the norms of the criminal procedure legislation of the Republic of Belarus and the Russian Federation, the practice of their application in forensic investigative activities, the article outlines both the tactical and forensic and procedural features of conducting an inspection of computer information in the disclosure and investigation of crimes.

In order to increase the efficiency of the inspection of computer information, it is proposed to amend the current criminal Procedure law of the Republic of Belarus aimed at additional regulation of the provisions related to the procedure for conducting this investigative action in a dwelling or other lawful possession. It is determined that the organization and tactics of this type of inspection, its effectiveness depend primarily on the characteristics of computer information and the means of protection used to protect it, as well as the technical equipment available in the arsenal of investigative bodies necessary for its detection, fixation and seizure.

Keywords: *criminal procedural activity, investigation, investigative inspection, tactics, computer information, information and telecommunication technologies, computer traces.*