ственности, если да, то за что именно; способно ли оказать сопротивление, покончить с собой, бежать; изучаются его образ жизни, распорядок дня, место учебы или работы; выясняются состояние здоровья, интересы, любимые занятия, личностные качества, черты характера обыскиваемого и членов его семьи, привычки и хобби, наличие в личном пользовании транспорта, если да, то какого, собаки или иных животных в жилом здании, оружия и т. д.

Таким образом, учитывая важность обыска, как наиболее значимого способа получения доказательственной информации, следователь должен обладать высокими профессиональными качествами, знаниями уголовно-процессуального законодательства, умело применять на практике криминалистические рекомендации по эффективному использованию в ходе обыска в жилище передовых информационных технологий, научно разработанных криминалистических тактических приемов и современных научно-технических и криминалистических средств, что позволит повысить результативность данного следственного действия.

УДК 343.98

И.В. Пашута

ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ОСМОТРА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Стремительное развитие информационно-телекоммуникационных технологий повлияло не только на широкое внедрение цифровых устройств в жизнь общества и каждого человека, но и на рост киберпреступлений (преступления против компьютерной безопасности, хищения имущества с использованием компьютерной техники, мошенничество и т. д.). В этой связи возросла актуальность исследования проблем, связанных с повышением эффективности деятельности органов уголовного преследования по установлению обстоятельств, значимых для расследования киберпреступлений, в процессе осмотра компьютерной информации, тактика которого имеет определенные особенности.

С криминалистической точки зрения осмотр компьютерной информации направлен на обнаружение, фиксацию, изъятие и обеспечение сохранности цифровых следов, находящихся в компьютерных устройствах. Рассмотрим наиболее сложные, на наш взгляд, вопросы, возникающие на подготовительном и рабочем этапах осмотра компьютерной информации.

На подготовительном этапе осмотра компьютерной информации наиболее важным, по нашему мнению, являются определение места проведения следственного действия и носителя компьютерной информации, научно-технических средств, необходимых для ее осмотра, решение вопроса о необходимости привлечения специалиста к участию в осмотре и некоторые другие.

Определяя место, где будет проводиться осмотр, следует исходить из того, что, во-первых, осмотр компьютерной информации может быть как составной частью осмотра места происшествия (труп, местность, помещение и т. д.), иного следственного действия (обыск, выемка, проверка показаний на месте и т. д.), так и самостоятельным следственным действием. Во-вторых, физически компьютерная информация неразрывно связана с ее носителем – оконечным (компьютерная система – персональный компьютер, ноутбук, планшет, смартфон и т. д.; машинный носитель – жесткий диск (HDD), твердотельный накопитель (SSD), флеш-карта и т. д.) или промежуточным (устройства, обеспечивающие функционирование компьютерной сети, – коммутатор, маршрутизатор (роутер), межсетевой экран и т. д.) электронно-цифровым устройством.

Среди научно-технических средств, необходимых для осмотра компьютерной информации, следует прежде всего выделить компьютерное оборудование и программное обеспечение (Cellebrite UFED 4PC, Belkasoft Evidence Center, «Элкомсофт», «Мобильный криминалист» и др.), предназначенные для обнаружения и анализа криминалистически значимой для расследования информации. Учитывая то, что в ходе проведения следственного действия в целях исключения возможного повреждения компьютерной информации может возникнуть необходимость в создании образа диска (побитной копии данных носителя), необходимо обеспечить наличие соответствующих аппаратно-программных средств или программ, таких как, например, EnCase, Acronis True Image и др. (позволяют проводить сбор, анализ и исследование интересующих данных без внесения каких-либо изменений в объект осмотра), а также носителей, на которые может быть перенесена обнаруженная компьютерная информация. Кроме того, целесообразно также установить наличие средств защиты компьютерной информации от несанкционированного доступа.

Привлечение специалиста для участия в следственном действии осуществляется путем заблаговременного направления письменного запроса от инициатора в адрес руководителя соответствующего органа или организации. К участию в проведении осмотра компьютерной информации могут привлекаться сотрудники подразделений по противодействию киберпреступности МВД Республики Беларусь, следователи криминалистических отделов Следственного комитета Республики Беларусь, сотрудники подразделений Государственного комитета судебных экспертиз Республики Беларусь и иные специалисты, имеющие соответствующее профильное образование (программист, тестировщик, инженер-программист и др.).

В следственных ситуациях, когда осмотр проводится без согласия собственника объекта осмотра (устройства, содержащего компьютерную информацию) при нем либо в его отсутствие, необходимо вынести постановление о проведении осмотра и получить санкцию прокурора.

На рабочем этапе осмотра компьютерной информации в целях исключения ее повреждения обязательно следует создать точную копию содержания носителя – образ диска, который в последующем будет использоваться в ходе следственного действия. Компьютерная информация по содержанию включает в себя различное программное обеспечение и личную информацию пользователя, которые представляют собой совокупность определенных файлов – именованных областей данных на носителе информации.

При осмотре работающего устройства следует определить, какая программа выполняется в данный момент, для чего необходимо осмотреть изображение на мониторе, описать его в протоколе и зафиксировать посредством фотосъемки и (или) видеозаписи. Если на устройстве используются программы, предназначенные для шифрования информации, либо программы, доступ к которым требует авторизации (при этом в момент осмотра доступ к ним открыт), то необходимо скопировать содержащуюся в них информацию на сторонний машинный носитель, после чего устройство отключить.

Фиксируя результаты осмотра компьютерной информации, в описательной части протокола необходимо отразить:

факт включения или выключения средств компьютерной техники на момент осмотра;

последовательность манипуляций, произведенных с устройствами в процессе осмотра средства компьютерной техники в целях поиска интересующей следствие информации, вплоть до перечисления нажимавшихся клавиш периферийных устройств, и полученные результаты;

наименование, условия и порядок использования аппаратных и программных средств, применяемых специалистами для обнаружения, исследования и изъятия следов преступлений, отметку о том, что указанные средства перед их применением были протестированы на предмет отсутствия в них вредоносных программ и закладок, перечень устройств, в которых применялись данные средства, полученные результаты;

сведения о файлах документов с указанием: названия файла, типа информации (текстовые, табличные, графические, аудио-, видеодокументы и т. д.), атрибутов (архивный, скрытый, системный, только для чтения, нет атрибутов), расположения на носителе (путь к файлу на логическом диске через папки-каталоги), размера и содержания хранимой информации, даты и времени создания и изменения.

В случае выявления вредоносных программ указываются: названия вредоносных программ; название, версия и наличие лицензии программы, диагностировавшей вредоносную программу, место запуска (диск того же компьютера, другого компьютера, компакт-диск); обозначение (номер) электронных носителей, на которые производилось копирование зараженных файлов, вредоносных программ, интересующих следствие.

По результатам осмотра компьютерной информации необходимо составить полный список папок, файлов и их реквизитов с помощью специальных программ каталогизации (программы формируют файл отчета, в который выводятся имя тома диска и серийный номер, список его каталогов и файлов, включая имена, дату и время последнего изменения; для файлов указываются расширение имени и размер; выводятся общее число файлов и каталогов, общий размер и размер свободного пространства на диске). При наличии принтера перечень содержимого каталогов (файлов) дисков следует распечатать.

Таким образом, учет изложенных обстоятельств в процессе осмотра органами уголовного преследования компьютерной информации позволит, как видится, в значительной степени оптимизировать работу по собиранию таких доказательств.

УДК 343.98

Н.Н. Пашута

ПРОВЕДЕНИЕ ПРОВЕРКИ ПО ЗАЯВЛЕНИЮ И СООБЩЕНИЮ О ПРЕСТУПЛЕНИИ: КРИМИНАЛИСТИЧЕСКИЙ АСПЕКТ

В современных условиях успешное осуществление задач уголовного судопроизводства напрямую зависит от того, насколько своевременно, законно и обоснованно принято уголовно-процессуальное решение. При этом защита прав личности, общества и государства от противоправных посягательств начинается с поступления в орган уголовного преследования информации о совершении общественно опасного деяния, предусмотренного уголовным законом, что обязывает принять необходимые меры, направленные на установление наличия либо отсутствия оснований для возбуждения уголовного дела.

Следует отметить, что уголовно-процессуальная деятельность по проверке заявления, сообщения о преступлении является определяющей и все другие виды деятельности (криминалистическая, оперативно-розыскная, экспертная) играют вспомогательную, обеспечивающую роль. В частности, как указывает Р.С. Белкин, криминалистическая деятельность наполняет процессуальную форму реальным деятельностным содержанием.

Вопросы, связанные с проверкой заявления, сообщения о преступлении, давно были предметом внимания как отечественных, так и зарубежных ученых в области уголовного процесса и криминалистики. Вместе с тем, анализируя специальную литературу, следует отметить, что криминалистические аспекты проведения такой проверки недостаточно освещены, несмотря на то что содержат ряд дискуссионных вопросов. Это обусловлено, помимо всего прочего, как отмечает А.Г. Филиппов, ошибочными суждениями некоторых криминалистов о том, что в доследственной проверке отсутствуют проблемные аспекты и в связи с этим нет необходимости в разработке тактических приемов и рекомендаций по ее проведению.

Несомненно, в правоприменительной практике имеются случаи, когда необходимость проведения проверки отсутствует и решение о возбуждении уголовного дела в соответствии с ч. 1 ст. 175 Уголовно-процессуального кодекса Республики Беларусь принимается незамедлительно. Однако во многих случаях, согласно статистическим сведениям, возбуждению уголовного дела предшествует проведение проверки в связи с отсутствием достаточных данных, указывающих на признаки преступления, наличие которых является одним из оснований для возбуждения уголовного дела.

По мнению большинства ученых, для принятия законного и обоснованного решения по заявлению, сообщению о преступлении необходимо установить достаточность данных, указывающих на такие признаки преступления, как общественная опасность (находит свое выражение в объекте и объективной стороне преступления) и противоправность (уголовно-правовая оценка деяния, по результатам которой может быть сформулирован вывод о наличии признаков конкретного преступления) деяния, при отсутствии обстоятельств, исключающих производство по уголовному делу.