объекта к вещественным доказательствам; О.Г. Григорьев придерживается точки зрения о том, что при установлении доказательственной значимости компьютерной информации, хранимой на носителе, следует выносить постановление о признании данного носителя информации вещественным доказательством), в другом – иными документами (В.В. Шалухин, Ю.А. Романов, ведя полемику по поводу иных документов, говорят о необходимости признания в качестве источников доказательств сведения, имеющиеся в информационных системах), в третьем – другими носителями информации (Р.В. Скачек относит к ним электронные источники доказательств и предлагает ввести новое следственное действие «применение программного обеспечения»).

Следует отметить, что каждый из исследователей по-своему прав. Однако системный взгляд на сущность, содержание и предназначение компьютерной информации в уголовном процессе, на наш взгляд, еще не выработан. Прежде всего нужно разобраться с технической составляющей вопроса. Необходимо четкое понимание того, с каким видом компьютерной (цифровой) информации имеет дело в каждом конкретном случае оперативный сотрудник или следователь, производящие расследование. Так, говоря об электронном документе, отображенном в письменном виде и удостоверенном соответствующей цифровой подписью, следует вести речь об одной из разновидностей источника доказательств – иные документы. Однако аутентичная (оригинальная) запись электронного документа находится в техническом устройстве, на котором был создан электронный документ. Изъятие машинного носителя компьютерной информации, оформленное соответствующим образом, последующий осмотр и экспертиза могут превратить его при определенных условиях в вещественное доказательство. Вместе с тем иногда возникает необходимость исследовать и само программное обеспечение, с помощью которого создавалась и обрабатывалась компьютерная информация. В этом случае, скорее всего, нужно вести речь о новом источнике доказательств, требующем процессуального закрепления в уголовно-процессуальном законе.

Изложенные подходы по рассматриваемым проблемам носят дискуссионный характер и требуют дальнейшего научного осмысления.

УДК 343.985

Н.Н. Беломытцев

НЕКОТОРЫЕ ОСОБЕННОСТИ ОСМОТРА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ДОСТУПА К НЕЙ

Преступления, совершаемые с использованием компьютерной информации, создают серьезную опасность для прав и интересов граждан, организаций и государства. Особую угрозу несут преступления, связанные с хищением имущества путем модификации компьютерной информации, так как могут причинять значительный материальный и моральный ущерб потерпевшим. Согласно статистическим данным в Республике Беларусь число таких хищений за шесть лет увеличилось в пять раз: с 3 585 в 2018 г. до 17 970 в 2022 г. При этом только 15,7 % уголовных дел, возбужденных по ст. 212 УК, были переданы в суд. Данным преступлениям характерны высокая степень латентности и низкие показатели раскрываемости. Один из шагов, направленных на борьбу с данными преступлениями, заключается в совершенствовании тактики осмотра компьютерной информации.

Осмотр компьютерной информации – это один из видов следственных действий, направленных на обнаружение, фиксацию и изъятие компьютерной информации в качестве доказательств по уголовному делу. Осмотр компьютерной информации предусмотрен ст. 204[1] УПК, которая определяет порядок, условия и границы его проведения. Однако, несмотря на нормативно-правовое регулирование, при проведении осмотра компьютерной информации практические сотрудники сталкиваются с рядом проблем и трудностей, обусловленных быстрым развитием информационных технологий, многообразием форм и способов совершения данных преступлений.

Изучение судебной и следственной практики показало, что данное следственное действие является наиболее распространенным. В 93,5 % исследованных уголовных дел, возбужденных по ст. 212 УК, проводился осмотр компьютерной информации. При этом осматривались различные источники электронно-цифровой информации, такие как стационарные и портативные компьютеры (персональные компьютеры, ноутбуки, моноблоки и т. д.); мобильные устройства (смартфоны, телефоны, планшеты, фотоаппараты, электронные книги, плееры, видеорегистраторы и т. д.); носители электронно-цифровой информации, включая жесткие диски (USB-флеш-накопители, HDD, SSD и др.), а также дампы (копии) носителей информации; телефонные и интернет-данные (сведения о персональных учетных записях и сообщениях в мессенджерах, социальных сетях, интернет-ресурсах, электронной почте, журналах регистрации событий от интернет-провайдера, дампах сетевого трафика телефонных соединений и т. д.); видеоданные (данные с видеокамер банкоматов, отделений банка, видеорегистраторов и т. д.); оперативно-розыскные данные (информация, полученная в ходе оперативно-розыскных мероприятий, таких как слуховой контроль, контроль в сетях электросвязи и т. д.); финансовые документы в электронном виде (квитанции об оплате, перечислении и переводе денежных средств, контрольные кассовые ленты, кассовые ордера, сведения о движении денежных средств по корреспондентскому счету и т. д.); сетевое оборудование (межсетевые экраны, маршрутизаторы, точки доступа, коммуникаторы и т. д.). В связи с разнообразием источников компьютерной информации, подлежащих осмотру, следователю необходимо учитывать особенности их исследования и обработки. При осмотре компьютерной информации нужно соблюдать следующие правила: привлекать специалиста по компьютерной технике и фиксировать его участие в протоколе (специалистом может выступать эксперт Государственного комитета судебных экспертиз, следователь криминалистического отдела Следственного комитета либо сотрудник подразделения ОВД по противодействию киберпреступности); использовать специальные программно-аппаратные комплексы (например, «Мобильный криминалист» или UFED) и носители информации

(например, оптические диски и др.) для копирования и сохранения компьютерной информации; осуществлять видеозапись экрана компьютерного устройства, чтобы зафиксировать все действия при осмотре (просмотр, копирование, выгрузка и т. д.), для этого необходимо устанавливать видеокамеру, направленную на экран устройства; копировать видеофайлы на носитель информации, упаковывать, приобщать к протоколу осмотра и опечатывать. Видеозапись должна отражать весь ход осмотра без пропусков и повторений по правилам криминалистической видеозаписи.

В некоторых случаях изъятие объекта, содержащего компьютерную информацию, имеющую значение для уголовного дела или материалов проверки, может быть невозможным или нецелесообразным. Например, если изъятие носителей информации нарушит работу организации или учреждения, где они являются частью инфраструктуры, а также в случаях, если нужно изъять определенную информацию, связанную с преступлением, но она находится на сервере, где также хранится огромный объем не связанных с ним данных, или находится в удаленном месте. В таких ситуациях при осмотре может осуществляться копирование компьютерной информации в отображаемой форме, в том числе создание побитового образа ее носителя. При этом необходимо соблюдать следующие требования: обеспечивать условия, исключающие возможность утраты, повреждения или изменения компьютерной информации при копировании; использовать процедуры и методы, гарантирующие достоверность и целостность копируемой компьютерной информации; фиксировать в протоколе осмотра факт копирования, указывая его вид, объем, время, место и способ копирования, а также характеристики носителя, на который копируется информация.

Подготовительный этап осмотра компьютерной информации включает в себя планирование его цели, задач, места, времени и способа. Цель и задачи зависят от мотивов и целей преступников, а также от обстоятельств совершения преступления. Мотивы и цели преступной деятельности могут быть разными: незаконное обогащение, уклонение от налогов, отмывание денег, получение конфиденциальной информации, месть, дезорганизация работы органов и организаций, сокрытие другого преступления, хулиганство, исследовательские цели, демонстрация личных способностей и т. д. Обстоятельства совершения преступления могут быть связаны с удаленным доступом, модификацией, копированием, уничтожением, хранением или передачей компьютерной информации. Целью данного осмотра является получение сведений о тех или иных фактах, входящих в предмет доказывания, либо других данных, представляющих интерес по уголовному делу.

Задачи осмотра могут быть следующими: изучение, выявление, фиксация и изъятие компьютерной информации; установление других источников доказательств; определение причинной связи между событиями преступления.

Место, время и способ осмотра определяются в зависимости от сложившейся ситуации и возможностей правоохранительных органов. Наиболее подходящим местом является кабинет сотрудника, проводящего осмотр, где есть необходимое оборудование. Осмотр обычно занимает длительное время. Способ осмотра компьютерной информации зависит от обстоятельств преступления, ее владельца, доступности места, где находится компьютерная техника, и т. д. Для осмотра привлекаются участники (подозреваемый (обвиняемый), свидетель, потерпевший, специалист и др.), технические средства (компьютерная техника с доступом в сеть Интернет, программно-аппаратные комплексы, видеокамера и т. д.) и др.

Возможны две типичные ситуации: когда имеется либо не имеется компьютерное устройство, связанное с преступлением. Первый случай можно разделить на следующие ситуации:

1. Пользователь сообщает данные для авторизации (входа) и соглашается на осмотр. В таком случае проводится осмотр и составляется протокол, в котором указываются участие и согласие пользователя, а также предоставленные им данные.

2. Данные для авторизации устанавливаются в ходе других процессуальных действий. Осмотр проводится с согласия пользователя или на основании постановления, санкционированного прокурором (если компьютерное устройство изъято в ходе следственных действий без санкции прокурора). При этом следует учитывать, что информация может быть зашифрована, скрыта, удалена или повреждена, что требует применения специальных программных средств для ее восстановления и дешифровки. Альтернативным способом решения задач в указанной ситуации является исследование компьютерного устройства и компьютерной информации в рамках проведения судебной компьютерно-технической экспертизы или судебной экспертизы радиоэлектронных устройств и электробытовых приборов.

3. Данные для авторизации отсутствуют. Осмотр проводится сотрудниками криминалистических отделов подразделений Следственного комитета по поручению следователя на основании постановления и в зависимости от обстоятельств изъятия компьютерного устройства, санкционированного либо не санкционированного прокурором. При необходимости сотрудник может обратиться за помощью к специалистам в области компьютерной техники или назначить проведение соответствующей экспертизы.

Во второй ситуации сотрудник не имеет компьютерного устройства, но может осмотреть информацию с использованием доступа в сеть Интернет (социальные сети, мессенджеры, электронная почта и т. д.), связанную с преступлением. Осмотр проводится на основании ч. 2 ст. 204^1 УПК с использованием служебного компьютера с доступом в сеть Интернет. Составляется протокол осмотра. Служебный компьютер не осматривается, а является научно-техническим средством доступа к данным.

Таким образом, осмотр компьютерной информации является эффективным способом получения доказательств по уголовным делам о хищении имущества путем модификации компьютерной информации. Для успешного проведения осмотра необходимо учитывать особенности доступа и обработки различных источников компьютерной информации, а также соблюдать правила и процедуры, установленные законодательством. Применение предложенного алгоритма действий способствует повышению качества и полноты осмотра, а также предотвращению потери или искажения доказательственной информации.