ленного возраста, а также изображение сексуальных действий с участием людей старше порогового возраста, которые имитируют или иным образом намекают на несовершеннолетие, даже если все участвующие лица достигли совершеннолетия.

Согласно Федеральному закону США детская порнография – это форма сексуальной эксплуатации детей, любое визуальное изображение откровенно сексуального поведения с участием несовершеннолетнего (фото-, видеоизображения, на которых запечатлен реальный несовершеннолетний либо анимационный персонаж).

Уголовный кодекс Канады приводит следующую формулировку термина «детская порнография» – любые объекты независимо от способа их создания, на которых изображено лицо, не достигшее 18 лет (либо имитирующее его) и вовлеченное в откровенную сексуальную деятельность, либо запечатлены в сексуальных целях половые органы или анальная область; пропагандирующие сексуальные действия с лицом в возрасте до 18 лет; любые письменные материалы либо аудиозапись, описывающие в основном сексуальную активность с лицом в возрасте до 18 лет.

В России дефиниция «порнографические материалы и предметы» закреплена ст. 242.1 УК, где в примечаниях имеется следующая формулировка: «под материалами или предметами с порнографическими изображениями несовершеннолетних… понимаются материалы и предметы, содержащие любое изображение или описание в сексуальных целях: полностью или частично обнаженных половых органов несовершеннолетнего; несовершеннолетнего, совершающего либо имитирующего половое сношение или иные действия сексуального характера; полового сношения или иных действий сексуального характера, совершаемых в отношении несовершеннолетнего или с его участием; совершеннолетнего лица, изображающего несовершеннолетнего, совершающего либо имитирующего половое сношение или иные действия сексуального характера».

В Республике Беларусь отсутствует единая общепринятая дефиниция для детской порнографии. Различные толкования данного термина имеются в некоторых официальных документах.

Например, в Положении о Республиканской экспертной комиссии по предотвращению пропаганды порнографии, насилия и жестокости, утвержденном постановлением Совета Министров Республики Беларусь от 22 октября 2008 г. № 1571, указывается, что «порнографические материалы или предметы порнографического характера с изображением несовершеннолетнего – разновидность порнографических материалов или предметов порнографического характера, которая включает в себя материалы или предметы, содержащие любое изображение или описание ребенка либо воспринимающиеся как изображение или описание ребенка либо совершеннолетнего лица, имитирующего ребенка, совершающего реальные или смоделированные действия сексуального характера либо принимающего участие в совершении таких действий или в их имитации, либо реалистичное изображение, в том числе созданное с использованием анимации или электронной техники, образа ребенка, совершающего или участвующего в совершении действий сексуального характера, а равно любое изображение или описание половых органов ребенка в сексуальных целях».

Республикой Беларусь 3 декабря 2001 г. также подписано соглашение «О присоединении Республики Беларусь к Факультативному протоколу к Конвенции о правах ребенка, касающемуся торговли детьми, детской проституции и детской порнографии».

Межпарламентская Ассамблея Содружества Независимых Государств (в состав которой входит Республика Беларусь) в 2008 г. постановила рекомендовать для использования в национальных законодательствах модельный закон от 3 апреля 2008 г. № 30-11«О противодействии торговле людьми». В ст. 3 этого закона понятие «детская порнография» раскрывается как «материалы или предметы, содержащие любые изображения или описания ребенка или совершеннолетнего лица, имитирующего ребенка, совершающего или имитирующего действия сексуального характера или принимающего участие в совершении таких действий или в их имитации, либо реалистичные изображения (в том числе созданные с использованием анимации и электронной техники) образа ребенка, совершающего или участвующего в совершении действий сексуального характера, а равно любое изображение или описание половых органов ребенка в сексуальных целях».

Исходя из вышеизложенного, полагаем необходимым законодательно закрепить в Республике Беларусь определение термина «детская порнография».

УДК 343.132 + 343.985

В.В. Бачила

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ОБЛАЧНЫХ ТЕХНОЛОГИЙ В ПРОЦЕССЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

Компьютерные технологии все активнее внедряются в повседневную жизнь современного общества. Весь европейский бизнес переходит на электронные документы, используемые в экономической деятельности. Они обеспечивают более быстрый обмен информацией между пользователями. При этом использование компьютерных технологий в преступных целях значительно осложняет работу правоохранительных органов по раскрытию и расследованию преступлений. Вместе с тем применение компьютерных технологий в деятельности оперативных сотрудников и следователей позволяет получить данные (сведения), которые могут быть использованы в процессе доказывания. Так, в мобильных устройствах часто содержится информация о связях подозреваемых или обвиняемых, их местонахождении в отдельных случаях, способах ведения бизнеса, применяемых мошеннических схемах. Все эти данные (сведения) помогают следователю расследовать преступление, совершенное с использованием компьютерных технологий. Еще более сложной является ситуация, когда преступники совершают противоправные действия при помощи современных облачных технологий.

Суть данной технологии заключается в том, что пользователь использует модель хранения данных в компьютерных сетях, когда информация размещается на различных серверах, которые могут находиться в разных странах. Для использования

облачного хранилища необходимо, чтобы в компьютерном устройстве была установлена соответствующая компьютерная программа, а также следует зарегистрироваться на сайте владельца облачных услуг, выбрав имя пользователя и пароль, указав, какую информацию необходимо загрузить в облачное хранилище. При этом следует учитывать то, что некоторые данные о пользователе загружаются в облако автоматически, без уведомления пользователя, после получения его согласия на синхронизацию устройства с одной из систем. Более того, хранилище может находиться в любой стране мира, тем самым затрудняя правоохранителям доступ к важной процессуальной информации. Еще одна проблема заключается в том, что в момент задержания лицо может одной несложной технической манипуляцией на мобильном носителе информации (смартфон, ноутбук и др.) уничтожить виртуальную информацию, хранящуюся в нем.

Таким образом, в ходе расследования преступлений возникает ряд трудностей, связанных с доступом к хранящейся в облаке информации пользователя, с ее грамотным процессуальным извлечением и закреплением (отражением в процессуальных документах, оформленных по результатам производства следственных и иных процессуальных действий).

Остановимся на следующих организационных и процессуальных проблемах, связанных с получением доступа, фиксацией, извлечением и процессуальным закреплением значимой для процесса расследования информации, хранящейся в облаке:

трудности, связанные с определением владельца информации и получением доступа к облачному хранилищу;

трудности, связанные с процессуальным статусом информации, полученной из облачного хранилища.

Суть первой проблемы заключается в том, что владельцы облачных технологий не несут ответственности за информацию, размещенную на их серверах третьими лицами, т. е. они не являются ее собственниками, несмотря на то что владеют машинными накопителями, на которых она хранится. Это приводит к тому, что без признательных показаний подозреваемого или обвиняемого о создании, использовании им информации, размещенной в облачном хранилище, и владении ею доказать факт принадлежности контента невозможно или крайне затруднительно. С практической точки зрения можно направить запрос владельцу облачного хранилища (находящегося в другой стране, в отдельных случаях в нескольких странах) о том, с какого IP-адреса интересующие данные загружены в облако, и тем самым доказать, что данные операции осуществил подозреваемый или обвиняемый. Однако, как правило, владелец облачного хранилища, ссылаясь на конфиденциальность данных своих пользователей, ответит отказом или вообще не отреагирует на запрос. В отдельных случаях владелец может указать на отсутствие соответствующих законодательных актов, заключенных между странами, об оказании правовой помощи в данных вопросах.

Кроме того, даже если будет получен доступ к мобильному устройству подозреваемого или обвиняемого, в котором содержится информация, идентичная хранящейся в облаке, он может заявить о том, что владельцем является другое лицо, к облаку которого произведено его подключение (доказать иное практически невозможно).

В целях доступа оперативного сотрудника или следователя к принадлежащему подозреваемому или обвиняемому средству компьютерной техники, с которого осуществляется доступ к облаку, необходимо получить добровольное согласие подозреваемого или обвиняемого на передачу логина (имя пользователя или адрес его электронной почты) и пароля. Согласие должно быть процессуально оформлено объяснением или протоколом допроса. Сложности начинаются при отказе подозреваемого или обвиняемого в доступе к компьютерным технологиям, в том числе облачным, в которых находится необходимая для следствия информация. В таких случаях используются силы и средства оперативно-розыскной деятельности.

Следующим шагом оперативного сотрудника или следователя будет проведение осмотра места происшествия, в ходе которого может быть проведен осмотр объекта (мобильного устройства), с которого осуществляется доступ к облаку (ст. 203, 204 УПК Республики Беларусь). При необходимости может быть произведено копирование компьютерной информации (ч. 3^1 ст. 204 УПК Республики Беларусь) или изъятие объекта, содержащего компьютерную информацию, с целью последующего осмотра в соответствии с положениями ст. 204^1 УПК Республики Беларусь. Производство указанных следственных действий целесообразно осуществлять с участием специалиста либо эксперта соответствующего профиля. По результатам произведенных следственных действий оформляются протоколы, в которых отражаются результаты осмотра. В отдельных случаях при изъятии мобильных компьютерных устройств или магнитных носителей информации целесообразно назначение проведения компьютерно-технической экспертизы.

При этом анализ полученных сведений и данных представляет собой хороший инструмент для расследования преступления, позволяющий собирать существующие облачные данные и метаданные, фиксировать и процессуально оформлять их таким образом, чтобы их можно было использовать в процессе доказывания.

Вместе с тем в уголовном процессе развернулась полемика по вопросу, к какому виду доказательств или источников доказательств относить данные (сведения), полученные с помощью компьютерных технологий.

Некоторые исследователи выдвигают аргументы в пользу того, что это новый вид доказательства (С. Фисюк говорит о необходимости введения в Хозяйственный процессуальный и Гражданский процессуальный кодексы Республики Беларусь нового вида доказательств – «информационно-вычислительные»; А.В. Казеев в 2019 г. вел речь о целесообразности внесения изменений в УПК Республики Беларусь в части, касающейся формулирования определения «электронного (цифрового) доказательства», однако в 2021 г. он скорректировал свою позицию и отнес их к источникам доказательств) или новые цифровые (электронные) источники доказательств (Н.А. Зигура считает необходимым выделить «компьютерную информацию» в самостоятельный источник доказательств; Н.А. Свирид рассматривает «электронный документ» как самостоятельный источник доказательств; А.Н. Першин выделяет «электронный носитель информации» в качестве нового источника доказательств; А.С. Рубис, Т.В. Ахраменко определяют в качестве нового источника доказательств «электронный документ» и предлагают внести соответствующие дополнения в ст. 88 УПК Республики Беларусь).

В свою очередь, ряд исследователей, обосновывая свою позицию, считают их в одном случае разновидностью вещественных доказательств (П.С. Пастухов не исключает отнесение компьютерной информации в силу специфики информационного

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