предварительно расследовано 43 362 уголовных дел, направлено в суд – 36 767, при этом до 72 % дел прекращаются либо приостанавливаются производством. Уровень раскрываемости таких киберпреступлений ниже в сравнении с общей раскрываемостью почти в два раза (21 % против 39,5 %).

Ущерб российской экономике от киберпреступлений превышает триллионы рублей и продолжает увеличиваться. Как правило, эти преступления совершаются в финансовой сфере. В то же время наблюдается значительное расширение использования информационно-коммуникационных технологий при совершении ряда иных уголовно наказуемых деяний, в том числе террористического и экстремистского характера, коррупционной направленности, преступлений против личности, половой неприкосновенности, иных охраняемых законом прав и законных интересов.

В основном органами Следственного комитета Российской Федерации осуществляется уголовное преследование по фактам совершения преступлений с использованием информационных технологий: против установленного порядка проведения азартных игр; в сфере незаконного оборота наркотических средств; связанных с изготовлением и распространением порнографических материалов; против половой неприкосновенности и половой свободы личности; экстремистской направленности.

Как показывает практика, киберпреступления часто носят транснациональный и трансграничный характер. Жертва и злоумышленник могут находиться на территории разных государств или даже континентов, а технологии позволяют им условно быть рядом.

Независимо от вида преступлений в качестве инструментов для их совершения используются ресурсы, размещенные на серверах в странах со сложным правовым порядком обмена информацией между правоохранительными органами. При этом для российских органов правоохраны по-прежнему основными инструментами получения данных из иных стран являются международная правовая взаимопомощь и каналы обмена информацией Национального центрального бюро Интерпола. Сроки получения ответов на запросы составляют от 6 до 24 месяцев, тогда как сроки хранения информации у большинства компаний, предоставляющих ресурсы для ее размещения на сервере, постоянно находящемся в сети (услуги хостинга), не превышают 6 месяцев. Таким образом, большинство запросов изначально не результативны.

К основным проблемам, связанным с оперативностью и качественными показателями расследования киберпреступлений, относятся:

разработка законодательства с учетом бумажного документооборота, а не высокоскоростного и трансграничного обмена данными;

различный подход государств к вопросам обмена данными, отсутствие единых стандартов, протоколов и т. д.;

монопольное владение основными ресурсами сети Интернет (социальные сети, корневые узлы сети, хостинг серверов) крупными корпорациями, находящимися в иной юрисдикции;

высокая латентность выявления и регистрации киберпреступлений;

низкие объемы и скорость обмена данными между правоохранительными органами и недостаточная их цифровизация;

отсутствие достаточного количества компетентных образовательных учреждений в сфере противодействия кибератакам и борьбе с киберпреступностью;

катастрофическая нехватка компетентных в раскрытии и расследовании киберпреступлений сотрудников правоохранительных органов;

высокая по скорости и существенная по содержанию мутация моделей угроз, способов использования технологий в противоправных целях;

рост количества квалифицированных высокоорганизованных преступных кибергрупп и сообществ, в том числе кибердиверсионных и террористических (занимаются телефонными минированиями, ложными новостями, направленными на подрыв доверия к власти и свержение государственного строя, и др.).

Неоспоримым фактором в решении этих проблем является формирование единого правового поля, которое будет содержать единый понятийный аппарат и подходы к сбору, фиксации, анализу и представлению цифровых доказательств, чтобы эффективно и максимально быстро взаимодействовать правоохранительным органам различных государств.

УДК 343.98

С.В. Кузьмина

ПРОБЛЕМЫ НАЗНАЧЕНИЯ И ПРОИЗВОДСТВА СУДЕБНЫХ ЭКСПЕРТИЗ ПО ДЕЛАМ О МОШЕННИЧЕСТВАХ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ

В условиях цифровизации практически любые виды преступлений, в том числе мошенничества, могут совершаться с помощью телекоммуникационных средств и систем. В связи с широким использованием информационно-телекоммуникационных технологий при совершении мошенничеств существенно изменились способы осуществления указанной преступной деятельности, а также следы, образующиеся в результате подготовки, совершения и сокрытия преступления. Указанные

изменения, безусловно, повлияли на методику расследования, вызвав необходимость совершенствования и разработки практических рекомендаций по осуществлению отдельных процессуальных действий, в частности назначения и производства судебных экспертиз по делам об интернет-мошенничествах.

По делам о мошенничествах, совершенных с использованием сети Интернет, назначаются и производятся различные виды экспертиз.

Наиболее часто по этим делам проводится компьютерная экспертиза для установления принадлежности исследуемого объекта к техническим средствам, а также для получения информации с технических средств в целях дальнейшего изучения.

Следует отметить, что в научной литературе и правовых актах указанная экспертиза также обозначается как компьютерно-техническая. Сторонники данного подхода в криминалистической науке предлагают выделять виды компьютерно-технической экспертизы в зависимости от объекта исследований: аппаратно-компьютерную, программно-компьютерную, информационно-компьютерную, компьютерно-сетевую [1, с. 110].

В ведомственных правовых актах МВД России, регулирующих деятельность экспертных подразделений органов внутренних дел, в частности в Перечне родов (видов) судебных экспертиз, производимых в экспертно-криминалистических подразделениях ОВД РФ, утвержденном приказом Министерства внутренних дел Российской Федерации от 29 июня 2005 г. № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации», рассматриваемая экспертиза обозначена как компьютерная судебная экспертиза, а в правовых актах Министерства юстиции РФ, регламентирующих вопросы проведения экспертиз, – как компьютерно-техническая судебная экспертиза (приказ Министерства юстиции Российской Федерации от 27 декабря 2012 г. № 237 (в ред. от 13 сентября 2018 г.) «Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым представляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России»). В связи с этим следователю при назначении экспертизы в части указания ее наименования в соответствующем постановлении необходимо руководствоваться нормативными актами того ведомства, которому будет поручено производство экспертизы.

С теоретической точки зрения считаем возможным согласиться с тем, что использование термина компьютерно-техническая экспертиза значительно сужает предмет данного исследования и не в полной мере отражает сущность экспертизы применительно к изучению компьютерной информации [2, с. 8]. Поэтому наиболее целесообразно использовать, на наш взгляд, термин «компьютерная экспертиза».

Объектами компьютерной экспертизы являются персональные компьютеры, периферийные, сетевые, запоминающие устройства и электронные носители данных.

В ходе компьютерной экспертизы по делам об интернет-мошенничествах подлежат разрешению вопросы, связанные с установлением: марки, модели, технических характеристик компьютерного или мобильного устройства; информации, содержащейся в памяти компьютерного устройства или носителе данных, в том числе информации о пользователе устройства (имена, пароли, права доступа); сведений о подключении к сети Интернет и конкретным сетевым ресурсам, об осуществлении электронной почтовой переписки; электронных платежей с использованием представленного на исследование устройства и др.

Производство компьютерной экспертизы предусматривает внешний осмотр представленных объектов, анализ их пригодности для исследования с помощью специализированного программного обеспечения (например, программы HDDScan для тестирования накопителей данных), принятие мер для блокирования возможности изменения данных носителя информации посредством специальных технических средств (блокираторов записи).

При производстве компьютерной экспертизы целесообразно осуществлять исследование копий цифровых объектов (образов) на тестовом компьютере эксперта, чтобы не нарушать целостность данных носителя-оригинала. Исследование информации непосредственно на носителе данных проводится только в случаях, если создание пригодной для экспертизы копии невозможно либо вид исследований физически не позволяет внести какие-либо изменения в информацию на оригинальном носителе.

Помимо компьютерной экспертизы актуальным направлением исследований, проводимых в ходе расследования интернет-мошенничеств, является судебная авторoведческая экспертиза текстов электронных сообщений, методика производства которой на сегодняшний день разработана в недостаточной степени. Специфика жанров интернет-коммуникации вызывает ряд методологических проблем при установлении авторства в ходе производства экспертизы.

Проблемными являются вопросы, связанные со сбором и предоставлением образцов для сравнительного исследования и с оценкой

идентификационных признаков применительно к сообщениям в сети Интернет [3, с. 60]. Полагаем, что при назначении и производстве авторoведческой экспертизы текстов веб-коммуникации нецелесообразно использовать экспериментальные образцы и свободные образцы письменной речи в связи с их жанровыми и стилевыми отличиями от текста интернет-сообщений. Представляется возможным использовать в качестве образцов для сравнительного исследования тексты личной электронной переписки, однозначно принадлежащей подозреваемому, что может быть подтверждено в результате компьютерной экспертизы, установления IP-адресов или кода IMEI для мобильных телефонов, а также в ходе допроса подозреваемого. Образцы переписки в сети Интернет предоставляются для исследования на материальном носителе в формате электронной страницы либо в виде скриншотов электронных страниц в целях сохранения своеобразия визуального (графического) оформления текста сообщения.

Еще одним проблемным при назначении и производстве авторoведческой экспертизы текстов веб-коммуникации является вопрос о достаточном и необходимом объеме интернет-сообщения для проведения идентификационных исследований. Полагаем, что такой объем должен определяться в каждом конкретном случае совместно с экспертом-авторoведом, исходя из специфики веб-коммуникации.

Значение авторoведческой экспертизы текстов веб-коммуникаций при расследовании мошенничеств, совершенных с использованием сети Интернет, заключается в возможности установления пола и возраста автора текста, его социально-психологических особенностей, а также в решении идентификационных задач, связанных с установлением автора конкретных сообщений.

При расследовании указанных преступлений могут проводиться и традиционные виды экспертиз, такие как почерковедческая, судебно-бухгалтерская, судебная экономическая (например, для анализа проводимых финансовых операций и отчетности при мошенничестве посредством создания интернет-магазина с регистрацией фиктивного юридического лица).

В некоторых случаях при расследовании интернет-мошенничеств возможно проведение психологической, комплексной психолого-психиатрической, психолингвистической экспертиз. При этом подобные экспертизы целесообразно проводить в отношении как обвиняемого, так и потерпевшего либо в рамках двустороннего исследования, поскольку процесс совершения киберпреступлений предполагает преднамеренные действия преступника, а также готовность потерпевшего откликнуться на оказываемое воздействие в ходе реализации различных способов мошенничества.

Таким образом, при расследовании мошенничеств, совершенных с использованием сети Интернет, назначаются и производятся как традиционные виды экспертиз, так и специфические, недостаточно изученные в криминалистической науке.

При назначении экспертиз по делам о расследовании мошенничеств, совершенных с использованием сети Интернет, и при постановке вопросов экспертам целесообразно проводить предварительные консультации с экспертами, а также изучать внутренние нормативные акты, регулирующие деятельность экспертных подразделений ведомства, которому будет поручено производство экспертизы, что особенно актуально для компьютерной экспертизы в связи с использованием различных наименований данного исследования в правовых актах.

1. Россинская Е.Р. К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности // Изв.Тул. гос. ун-та. Эконом. и юрид. науки. 2016. Вып. 3, ч. 2. С. 109–117.

2. Аверьянова Т.В. Вопросы интеграции и дифференциации научных знаний в криминалистике и судебной экспертизе // Актуальные проблемы криминалистики на современном этапе : материалы междунар. конф., посвящ. памяти проф. Л.Л. Каневского, 23–24 янв. 2003 г. : в 2 ч. Уфа, 2003. Ч.1. С. 3–9.

3. Мирошниченко М.Р. Проблемы производства судебной авторoведческой экспертизы текстов Интернет-коммуникации // Вектор науки Тольят. гос. ун-та, Серия «Юрид. науки». 2016. № 1. С. 59–62.

УДК 343.9

А.И. Лавникович

ПРИЧИНЫ ПРЕСТУПНЫХ НАРУШЕНИЙ ПРАВИЛ ДОРОЖНОГО ДВИЖЕНИЯ И МЕРЫ ИХ ПРЕДУПРЕЖДЕНИЯ

В научной литературе причины дорожно-транспортных происшествий (ДТП) принято делить на две основные группы: объективные (конструктивные параметры и состояние дороги, техническое состояние транспорта, интенсивность движения транспортных средств и пешеходов, обустройство дорог сооружениями и средствами регулирования, погодные условия, время года и т. д.) и субъективные (состояние участников дорожного движения, нарушение установленных правил водителями и пешеходами, недостаточная профессиональная подготовка водителя) [1, с. 7].