6. Шумилов А. Ю. Оперативно-разыскная наука в Российской Федерации : в 3 т. : монография / А. Ю. Шумилов. — М. : Изд. дом Шумиловой И.И., 2013. – Т. 1. – 455 с.

Информация об авторе

Драпезо Роман Григорьевич – старший преподаватель кафедры уголовного процесса и криминалистики юридического факультета Кемеровского государственного университета, 650043, г. Кемерово, пр. Советский, 73 (ауд. 2201, деканат юридического факультета), e-mail: uri_nit@kemsu.ru.

Information about the author

Drapezo Roman Grigoryevich – the senior teacher of chair of criminal trial and criminalistics of law department of the Kemerovo state university, 650043, Kemerovo, Sovetsky Ave., 73 (a miss. 2201, dean's office of law department), e-mail: uri_nit@kemsu.ru.

УДК 343.9:343.72
ББК 67.52:67.408.121

В.В. Коломинов
И.Г. Смирнова

К ВОПРОСУ О ФОРМИРОВАНИИ КРИМИНАЛИСТИЧЕСКОГО ЗНАНИЯ О МОШЕННИЧЕСТВЕ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ*

В статье авторы делают акцент на распространенности и серьезности угрозы мошенничества в сфере компьютерной информации, необходимости использования следователем в процессе раскрытия и расследования таких преступлений криминалистических знаний об элементах механизма их совершения. Анализируя отдельные элементы механизма преступления, авторы обращают внимание на их взаимосвязь между собой, их специфические особенности. Отмечается роль элементов, касающихся компьютерной информации, компьютерных средств, механизма следообразования в формировании криминалистического знания при расследовании обозначенных преступлений.

Ключевые слова: киберпреступность; компьютерные преступления; мошенничество в сфере компьютерной информации, механизм преступления.

* Материал подготовлен в рамках выполнения проекта «Повышение эффективности уголовного судопроизводства по делам о киберпреступлениях для обеспечения национальной безопасности» в рамках гранта Президента Российской Федерации для государственной поддержки молодых российских ученых – докторов наук (Конкурс – МД-2014) на 2014-2015 годы (договор № 14.Z56.14.2691-МД).

V.V. Kolominov
I.G. Smirnova

ISSUES ON THE FORMATION OF THE CRIMINAL KNOWLEDGE ABOUT FRAUD IN THE FIELD OF THE COMPUTER INFORMATION

In this article the author focuses on the prevalence and the serious danger of fraud and depict that it is necessary for investigator to use criminal knowledge about mechanisms' elements of these crimes in disclosure and investigation procedures. Analyzing the individual elements of the crime's mechanism the author pays attention to their connection with each other and their specific features. Also the problem of some elements concerning with the computer information, computer tools, mechanisms of the trace-reminds in the formation of the criminalistic knowledge in these crimes investigation is razed in this paper.

Keywords: cybercrime; computer crimes; fraud in the field of the computer information.

Развитие компьютерных технологий вызвало появление и активное распространение таких общественно опасных преступлений, как мошенничество в сфере компьютерной информации. При установлении механизма такого мошенничества необходимо учитывать ряд элементов и признаков, знания о которых необходимы следователю в процессе выявления, раскрытия и расследования таких деяний. Знания о каждом из этих элементов, обладающих характерными особенностями, ложатся в основу формирования криминалистического знания о расследуемом факте мошенничества и составляют криминалистически значимую информацию о данных преступлениях.

Проанализируем отдельные элементы механизма мошенничества в сфере компьютерной информации с целью определения их взаимодействия между собой и влияния каждого из них на формирование криминалистических знаний о противоправном деянии.

Прежде всего, необходимы знания о компьютерных средствах. Как следообразующие объекты компьютерные средства выступают в двух аспектах:

– как носители информации об объективной стороне преступного деяния;

– как носители информации о самом субъекте преступления. Особенность заключается в том, что компьютерные средства сами не выступают следами преступной деятельности, так как не обладают характерными специфическими особенностями, но при этом несут на себе следовую картину преступного деяния. Об этом свидетельствует анализ следственной практики, когда, например, при производстве следственных действий, из компьютера изымается только его «жесткий диск» – запоминающее устройство для хранения информации. Между тем, технические характеристики компьютерно-технических средств и их наличие или отсутствие вообще должны свидетельствовать о возможности реализации преступного умысла (например, наличие или отсутствие подключения компьютера к телекоммуникационной сети).

Большинство ученых сходятся во мнении, что основной характерной особенностью компьютерно-технических средств, с проекцией на потребности расследования, является их свойство сохранять информацию. С этим следует согласиться так, как это и является определяющим моментом формирования криминалистического знания о компьютерных преступлениях и, в частности, такого вида, как мошенничество в сфере компьютерной информации.

К источникам компьютерной информации относятся системы, компоненты которых обеспечивают размещение, доступность, а также целостность сведений, составляющих информацию. Это:

– постоянное запоминающее устройство компьютера (ПЗУ) – его внутренняя память, включающая несколько микросхем, постоянно хранящих определенную информацию;

– оперативное запоминающее устройство (ОЗУ) – оперативная память, содержащая информацию, необходимую для работы компьютера;

– сверхоперативная память (кэш) – сверхбыстродействующие микросхемы памяти – кэш-память для повышения производительности компьютера.

Существуют также внешние источники – внешняя (долговременная) память, предназначенная для долговременного хранения программ и данных, не используемых в данный момент, которая требует наличие устройства, обеспечивающего запись/считывание информации – накопителя или дисковода, а также устройства хранения информации – носителя. К ним относятся накопители на оптических компакт-дисках (CD-R/RW, DVD-R/RW); флэш-накопители (MMC Plus (Multimedia Card), SD Mini (Secure Digital), SD Micro (Secure Digital), MS Pro (Memory Stick Pro), MS Pro Duo (Memory Stick Pro Duo), CF (Compact Flash), SD (Secure Digital) и др.

Таким образом, средства накопления криминалистически значимой информации представляют собой довольно сложные объекты – компьютеры (устройства), состоящие из множества элементов, а также средства накопления, обработки и хранения информации.

Следует заметить, что привести полный перечень таких устройств в настоящее время достаточно затруднительно в связи с быстрым темпом научно-технического прогресса в области компьютерных технологий и появлением новых форм накопителей. Однако, поскольку указанные объекты имеют специфические свойства, и характер функционирования их следует учитывать при разработке практических рекомендаций по расследованию мошенничества в сфере компьютерной информации.

Интерес для формирования криминалистического знания об исследуемом виде мошенничества представляют также компьютерные сети. По мнению В.П. Косарева и Л.В. Еремина компьютерная сеть – это совокупность компьютеров, между которыми возможен информационный обмен без промежуточных носителей информации [3, с. 440].

Подобное суждение выглядят не бесспорным, поскольку в данном определении не в полной мере отражена техническая особенность передачи данных в сети. Авторы акцентируют внимание лишь на наличии промежуточных звеньев в сети при передаче информации. Вместе с тем к промежуточным звеньям

при передаче информации можно отнести различные носители информации (например, переносные жесткие диски, USB флэш-карты, лазерные CD, DVD диски и т. п.). При этом их наличие или отсутствие предопределяет тип компьютерной системы, которая, в свою очередь, может включать как автономные вычислительные системы, так и их сети.

Таким образом, нельзя назвать компьютерной сетью систему, которая не включает в себя помимо рабочих станций (технически сложных устройств, например, компьютера, смартфона, компактного персонального компьютера (КПК), планшетного персонального компьютера и т. п.), посредством которого пользователь (абонент) получает доступ к ресурсам компьютерной сети) каких-либо промежуточных накопителей информации.

Следовательно, особенностью компьютерных сетей является то, что их существует несколько видов и в зависимости от территориальной распространенности делятся на:

– локальные компьютерные сети (ЛВС, LAN-Local Area Network) (создаются и используются юридическими лицами, как правило, в пределах своего размещения, либо физическими лицами в обособленной административно-территориальной единице);

– региональные компьютерные сети (РВС, MAN – Metropolitan Area Network), связывающие абонентов района, города, области;

– глобальные компьютерные сети (ГВС, WAN – Wide Area Network), соединяющие абонентов, удаленных друг от друга на любое расстояние.

Наиболее распространенной, безусловно, является всемирная глобальная сеть Интернет. При этом анализ изученных материалов уголовных дел о преступлениях, совершаемых в сфере компьютерной информации, свидетельствует, что для совершения таких деяний в 95 % случаев использовались глобальные компьютерные сети, в 4 % случаях региональные и лишь в 1 % случаях локальные компьютерные сети.

Таким образом, любые компьютерные сети также имеют свои характерные криминалистические особенности, и, по сути, могут эффективно использоваться субъектами преступной деятельности в целях совершения мошенничества. При этом, характерной особенностью компьютерных сетей, как орудия и средства совершения исследуемого мошенничества является то, что они также содержат следы осуществления операций, направленных на реализацию преступного замысла. Например, независимо от отправляющего и принимающего устройства, в электронной почте хранятся электронные письма, отправленные и принятые на определенный адрес и т. п. Зная свойства и принцип работы телекоммуникационной сети, следователь или лицо, производящее дознание, способны обнаружить в ней значительный объем информации о преступном деянии. Компьютерная сеть также является средством передачи информации между абонентами сети.

Нельзя не подчеркнуть, что практически все формы незаконной деятельности, имеющие место в сфере компьютерной информации, в том числе мошенничество, осуществляются с использованием различных программ, разработка и внедрение в компьютерную систему которых является средством обеспечения совершения преступлений.

В процессе расследования исследуемых преступлений следует учитывать, что подготовка, написание, тестирование специальных компьютерных программ для взлома, внедрение вредоносных «троянских» программ, программ-шпионов, поиск паролей или определение способов беспарольного входа будет оставлять виртуальные следы в памяти компьютера или иного технически сложного устройства, используемого мошенником. При этом примененные способы воздействия на компьютер «жертвы» будут аналогичным образом оставлять следы в памяти ее компьютера.

Как справедливо отмечает А. Смушкин, для указанных преступных действий могут использоваться программы различного уровня сложности: «стандартные» – которые составлены максимально просто и которые легко найти в сети Интернет или в специальной области закрытого участка Интернет; «приспособленные» программы – переделанные самим злоумышленником под свои нужды; самостоятельно написанные злоумышленником программы [2, с. 43–45].

Рассматривая вопросы формирования криминалистических знаний о мошенничестве в сфере компьютерной информации, отдельными учеными предлагаются новые варианты определения понятия и механизма следообразования. Однако, на наш взгляд, к этому надо подходить достаточно осторожно. Так, П.В. Мочагин, предлагает к двум традиционным формам отражения следообразования – материально-фиксированной и идеальной, добавить еще одну – в виртуально-информационной и технико-компьютерной сфере [1, с. 97]. Данная позиция представляется достаточно спорной, поскольку специфика образования, обработки и хранения компьютерной информации предусматривает использование для этих целей вполне материальных средств (компьютерно-технических). Именно это обстоятельство предусматривает возможность материально-фиксированного отображения компьютерной информации на носителях указанных средств.

Следовательно, в качестве следов мошенничества в сфере компьютерной информации вполне можно рассматривать электронные сигналы (команды), отправленные с компьютера субъекта преступной деятельности, которые предаются по телекоммуникационным сетям с целью хищения чужого имущества или приобретения права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Эти сигналы имеют точки начала и окончания их движения (имеются в виду компьютеры, между которыми они предаются), а они, в конечном итоге, имеют материально-фиксированное выражение – персональный компьютер или иное технически сложное устройство, его IP-адрес.

В криминалистической литературе такие следы предлагается именовать информационными или виртуальными, и в том виде, в котором их представляют ученые, они являются, не чем иным, как материальными следами-отображениями. Обусловлено это тем, что они имеют вполне материально-фиксированное отражение на материальных носителях, именно это позволяет их идентифицировать с помощью разработанных наукой средств и методов. Иначе такой подход, предложенный учеными, на наш взгляд, позволял бы го-

ворить о таких видах следов, как военные следы (по делам о военных преступлениях), террористических следах (по делам о терроризме), технических следах и т. п. Такой подход способствовал бы лишь загромождению разработанных криминалистикой знаний о рассматриваемых проблемах.

В заключение еще раз отметим, что формирование криминалистического знания о мошенничестве в сфере компьютерной информации представляет собой процесс исследования механизма преступления и его отдельных элементов. Механизм мошенничества в сфере компьютерной информации закономерно обусловливает возникновение криминалистически значимой информации о самом преступном хищении чужого имущества или приобретении права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, его участниках и результатах. При этом познание и систематизация криминалистических признаков совершения данного вида мошенничества позволяет разработать научные положения и разрабатываемые на их основе практические рекомендации по расследованию данной деятельности.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Мочагин П. В. Новые формы следообразований в криминалистике и судебной экспертизе / П. В. Мочагин // Судебная экспертиза в парадигме российской науки : (к 85-летию Ю. Г. Корухова) : сб. материалов 54-х криминал. чтений : в 2 ч. – М. : Акад. управления МВД России, 2013. – Ч. 2. – С. 97–101.

2. Смушкин А. Виртуальные следы в криминалистике / А. Смушкин // Законность. – 2012. – № 8. – С. 43–45.

3. Экономическая информатика / под ред. В. П. Косарева, Л. В. Еремина. – М. : Финансы и статистика, 2001. – 592 с.

Информация об авторах

Коломинов Вячеслав Валентинович – преподаватель кафедры криминалистики и судебных экспертиз, Байкальский государственный университет экономики и права, 664003, г. Иркутск, ул. Ленина, д. 11, e-mail: OffRoad88@mail.ru.

Смирнова Ирина Георгиевна – доктор юридических наук, заведующая кафедрой криминалистики и судебных экспертиз, Байкальский государственный университет экономики и права, 664003, г. Иркутск, ул. Ленина, д. 11, e-mail: smirnova-ig@mail.ru.

Information about the authors

Kolominov Vyacheslav Valintinovich – teacher of the department of criminalistics and judicial examinations, Baikal National University of Economics and Law, Lenin st., 11, Irkutsk, 664003, e-mail: OffRoad88@mail.ru.

Smirnova Irina Georgievna – Doctor of Law, Professor, head of the department of criminalistics and judicial examinations, Baikal National University of Economics and Law, 11, Lenin str., Irkutsk, 664003, e-mail: smirnova-ig@mail.ru.

УДК 343.985
ББК 67.523.14

В.С. Кряжев

ОПЕРАТИВНО-РОЗЫСКНЫЕ И ИНЫЕ МЕРОПРИЯТИЯ, ИСПОЛЬЗУЕМЫЕ В ЦЕЛЯХ БОРЬБЫ С ПРЕСТУПЛЕНИЯМИ ТЕРРОРИСТИЧЕСКОЙ И ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ

В статье рассматриваются меры, направленные на повышение эффективности проведения оперативно-розыскных мероприятий и следственных действий по уголовным делам, связанным с преступлениями террористической и экстремистской направленности.

Ключевые слова: оперативно-розыскные мероприятия, терроризм, экстремизм.

V.S. Kryazhev

OPERATIVELY-SEARCHING ACTIONS, USED IN ORDER TO DEAL WITH THE CRIMES OF TERRORIST AND EXTREMIST ORIENTATION

The article describes the actions, directed to increase the efficiency of the operatively-searching actions and the investigation of criminal cases, related to the crimes of terrorist and extremist orientation.

Keywords: operatively-searching actions, terrorism, extremism.

За последние несколько десятков лет феномен экстремизма значительно изменился в худшую сторону. И соответственно, как его крайнее проявление – терроризм, претерпел ряд изменений как качественного, так и количественного характера. На сегодняшний день в России, как и во многих других странах, это является фактором глобального значения.

В ходе раскрытия, расследования и предупреждения преступлений террористической и экстремистской направленности широко используются средства оперативно-розыскной работы. Это конечно же широкий спектр оперативно-розыскных мероприятий и иных организационных действий. Специфика ОРД по уголовным делам данной категории или специфика работы в ходе доследственной проверки сообщений о преступлениях, а также иные способы выявления этих преступлений связаны в том числе и с умелым использованием АИПС.