УДК 343.9:343.72
DOI 10.17150/2072-0904.2015.6(1).26

В. В. Коломинов
Байкальский государственный университет экономики и права,
г. Иркутск, Российская Федерация

МОШЕННИЧЕСТВО В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: КРИМИНАЛИСТИЧЕСКИЙ АСПЕКТ

Аннотация. Федеральным законом от 29 ноября 2012 г. № 207-ФЗ было криминализировано деяние и предусмотрена уголовную ответственность за совершение мошеннических действий в сфере компьютерной информации. В статье сделан акцент на распространенности и серьезности угрозы мошенничества в сфере компьютерной информации, необходимости использования следователем в процессе раскрытия и расследования преступлений криминалистических знаний об элементах механизма их совершения. Раскрывается значение компьютерных средств как следообразующих объектов, выступающих в качестве носителя информации об объективной стороне преступного деяния и его субъекте преступления. Анализируются отдельные элементы механизма преступления и обращается внимание на их взаимосвязь между собой и 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.

Информация о статье. Дата поступления 5 декабря 2014 г.; дата принятия к печати 29 декабря 2014 г.; дата онлайн-размещения 26 января 2015 г.

Финансирование. Договор № 14.Z56.14.2691-МД об условиях использования гранта Президента Российской Федерации для государственной поддержки молодых российских ученых с организациями — участниками конкурсов, имеющими трудовые отношения с молодыми учеными, МД-2691.2014.6.

V. V. Kolominov
Baikal State University of Economic and Law,
Irkutsk, Russian Federation

FRAUD IN THE FIELD OF COMPUTER INFORMATION: CRIMINALISTIC ASPECT

Abstract. The federal law of November 29, 2012 No. 207-ФЗ criminalizes the act and envisages criminal liability for committing fraud in the sphere of computer information. The article lays stress on the abundance and seriousness of fraud threat in the sphere of computer information on the necessity of using criminalistic knowledge of elements of the crime commission mechanism by the investigator in the process of detecting and investigating crimes. It reveals the importance of computer tools trace-making objects serving as information carrier of information about the objective side of the criminal action and its subject of the crime. It analyses separate elements of the crime mechanism and draws attention to their interrelation and specific features and notes the role of the elements concerning computer information, mechanism of trace-making in forming knowledge while investigating the specified crimes.

Keywords. Cyber crime; computer crimes; fraud in the field of computer information; mechanism of crimes.

Article info. Received December 5, 2014; accepted December 29, 2014; available online January 26, 2015.

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2015. Т. 6, № 1
http://eizvestia.isea.ru

Financing. The material was prepared in the framework of implementing the agreement on the conditions of using of the grant of the President of the Russian Federation for the state support of young Russian scientists with organizations — participants of the competition, having work relationship with young scientists No. 14.Z56.14.2691-MD (MD-2691.2014.6).

«Анализ... характеристик любого явления... предполагает закономерное обращение к социально значимым понятиям, общественным характеристикам изучаемого явления» [2, с. 144].

Развитие компьютерных технологий вызвало появление и активное распространение таких общественно опасных преступлений, как мошенничество в сфере компьютерной информации. При установлении механизма подобного мошенничества необходимо учитывать ряд элементов и признаков, знания о которых необходимы следователю в процессе выявления, раскрытия и расследования таких деяний. Полученные сведения 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 являются 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, подключение или неподключение 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, потому что это и есть определяющий момент 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:

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

– оперативное запоминающее устройство — оперативная память, содержащая информацию, необходимую для работы компьютера;

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

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2015. Т. 6, № 1
http://eizvestia.isea.ru

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, то 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 [4, с. 440]. Подобное суждение выглядят не бесспорным, поскольку в данном определении не в полной мере отражена техническая особенность передачи данных в сети. Автор акцентирует 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 и флеш-карты, лазерные CD, DVD диски и т. д.). 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 или планшетного персонального компьютера, 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 они делятся на сети:

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

– глобальные компьютерные (ГВС, WAN — Wide Area Network), соединяющие абонентов, удаленных друг от друга на любом расстоянии.

Наиболее распространенной, безусловно, является всемирная глобальная сеть Интернет. При этом анализ изученных материалов уголовных дел

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2015. Т. 6, № 1
http://eizvestia.isea.ru

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2015. Т. 6, № 1
http://eizvestia.isea.ru

о преступлениях, совершаемых в сфере компьютерной информации, свидетельствует, что для совершения таких деяний в 95 % случаев использовались глобальные компьютерные сети, в 4 % — региональные и лишь в 1 % — локальные компьютерные.

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. 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» — составлены максимально просто и их легко найти в сети Интернет или в специальной области закрытого участка Интернет; «приспособленные» — переделанные самим злоумышленником под свои нужды; самостоятельно написанные [3, 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 — виртуально-информационную и технико-компьютерную сферу [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 пре-

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2015. Т. 6, № 1
http://eizvestia.isea.ru

даются 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. У этих сигналов есть 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 говорить о таких видах следов, как военные следы (по делам о военных преступлениях), террористические следы (по делам о терроризме), технические следы и т. д. Подобный 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 позволяют разработать научные положения и создаваемые 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 кримин. чтений : в 2 ч. — М. : Академия управления МВД России, 2013. — Ч. 2. — С. 97–101.

2. Смирнова И. Г. Ценность как основная категория аксиологии и ее значение в праве / И. Г. Смирнова // Известия Иркутской государственной экономической академии. — 2010. — № 5 (73). — С. 144–148.

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

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

References

1. Mochagin P. V. New forms of trace-making in criminalistics and forensic inquiry. *Sudebnaya ekspertiza v paradigme rossiiskoi nauki (k 85-letiyu Yu. G. Korukhova)* [Forensic Inquiry in the paradigm of the Russian science (to the 85-th Anniversary of

Yu. G. Korukhov)]. Moscow, Academy of Management of MIA of Russia Publ., 2013, part. 2, pp. 97–101. (In Russian).

2. Smirnova I. G.Value as a main category in axiology and its meaning in law. *Izvestiya Irkutskoy gosudarstvennoy ekonomicheskoy akademii = Izvestiya of Irkutsk State Economics Academy*, 2010, no. 5 (73), pp. 144–148. (In Russian).

3. Smushkin A. Virtual traces in criminalistics. *Zakonnost' = Legalism*, 2012, no. 8, pp. 43–45. (In Russian).

4. Kosarev V. P., Eremin L. V. (ed.). *Ekonomicheskaya informatika* [Economic Informatics]. Moscow, Finansy i statistika Publ., 2001. 592 p.

Информация об авторе

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

Author

Vyacheslav V. Kolominov — Senior Lecturer, Chair of Criminalistics and Forensic Inquiry, Baikal State University of Economics and Law,11 Lenin St., 664003, Irkutsk, Russian Federation; e-mail: OffRoad88@mail.ru.

Библиографическое описание статьи

Коломинов В. В. Мошенничество в сфере компьютерной информации: криминалистический аспект / В. В. Коломинов // Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права). — 2015. — Т. 6, № 1. — URL : http://eizvestia.isea.ru/reader/article.aspx?id=19976. — DOI: 10.17150/2072-0904.2015.6(1).26.

Reference to article

Kolominov V. V. Fraud in the field of computer information: criminalistic aspect. *Izvestiya Irkutskoy gosudarstvennoy ekonomicheskoy akademii* (*Baykalskiy gosudarstvennyy universitet ekonomiki i prava*) = *Izvestiya of Irkutsk State Economics Academy* (*Baikal State University of Economics and Law*), 2015, vol. 6, no. 1. Available at: http://eizvestia.isea.ru/reader/article.aspx?id=19976. DOI: 10.17150/2072-0904.2015.6(1).26. (In Russian).

http://eizvestia.isea.ru
2015. Т. 6, № 1
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ