УДК 343.98

В.В. Коломинов

МОШЕННИЧЕСТВО В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ КАК ОБЪЕКТ КРИМИНАЛИСТИЧЕСКОГО ПОЗНАНИЯ*

Федеральным законом от 29.11.2012 г. №207-ФЗ была криминализирована статья, предусматривающая уголовную ответственность за совершение мошеннических действий в сфере компьютерной информации. В статье анализируются признаки данных преступлений, которые являются объектом криминалистического исследования и способы совершения мошеннических действий.

Ключевые слова: мошенничество в сфере компьютерной информации, информационные системы, компьютерная сеть, телекоммуникационная сеть, киберпреступность.

V.V. Kolominov

SWINDLE IN THE FIELD OF COMPUTER INFORMATION AS OBJECT OF CRIMINALISTICS COGNITION

Federal law from 29.11.2012 №207-FZ city has criminalized an article providing for criminal liability for committing fraud in the sphere of computer information. The article analyzes the characteristics of these crimes, which are the subject of forensic investigation and ways of committing fraud.

Keywords: fraud in the sphere of computer information, information systems, computer network, telecommunications network, cybercrime.

Федеральным законом от 29.11.2012 г. №207-ФЗ в уголовное законодательство была введена статья 159.6 УК РФ, предусматривающая ответственность за мошенничество в сфере компьютерной информации. Данное мошенничество представляет собой хищение чужого имущества или приобретение права на чужое имущество путем

* 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).

ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Процесс расследования преступлений в сфере компьютерной информации предусматривает необходимость производства значительного числа регламентированных процессуальным законом следственных и иных процессуальных действий [7, с. 2].

Как известно, при расследовании преступлений необходимо разрешить вопрос о том, что подлежит установлению и доказыванию в каждом конкретном случае. В этой анализ следственной и судебной практики показывает, что определенную сложность при расследовании мошенничества в сфере компьютерной информации представляет установление такого обстоятельства, подлежащего доказыванию как «место совершения преступления».

В уголовно-процессуальной литературе неоднократно подчеркивалось значение предмета доказывания в предварительном расследовании и судебном разбирательстве по уголовному делу. Как справедливо отмечено М.С. Строговичем: «верное определение содержания предмета доказывания обеспечивает целенаправленность и плановость действий следователя, прокурора и суда» [8, с. 361].

Место преступления в криминалистике традиционно определяется как место, в котором реализуется объективная сторона преступления – место преступления, участок местности или помещение, где было совершено преступление [1, с. 115]. В нашем случае также представляется необходимым, в том числе рассматривать понятие места происшествия, под которым понимается, участок местности или помещение, где были обнаружены следы события, требующего расследования.

Одной из основных особенностей рассматриваемого элемента криминалистического знания о событии преступления является то, что место совершения преступления оказывает влияние на весь процесс формирования следовой картины и, соответственно, является носителем, как материальных, так и идеальных следов, а значит, обладает существенной информативностью.

Как отмечает Л.Г. Видонов: «главной характеристикой места преступления являются его признаки, определяющие его назначение для людей и отличающие его от окружающей местности и обстановки» [2, с. 11].

Необходимо отметить, что признаки и свойства места совершения мошенничества в сфере компьютерной информации имеют определяющее значение для разработки практических рекомендаций по его установлению в ходе расследования, а также их использованию в процессе установления обстоятельств преступного деяния. Это обусловлено рядом следующих обстоятельств. Прежде всего, компьютерная информация предусматривает необходимость ее обработки, хранения и обмена, а для этого необходимо наличие компьютерных средств и средств обмена информацией, т.е. сети.

Характерной особенностью, имеющей определяющее значение для возможности контроля движения информации в сети, по мнению И.Н. Воробец, является то, что: «Система адресации в сети Интернет описываемая IP-протоколом, построена на основе присвоения каждому компьютеру, подключенному к Сети, уникального идентификационного номера (IP-адреса). IP-адрес – это набор из четырех десятичных чисел, отделенных точками (например, 192.168.100.47.). Для удобства работы числовые адреса заменяются символьными с использованием доменной системы преобразования имен. Система доменов позволяет преобразовывать символьные имена в IP-адреса и обратно определять имя домена по числовому адресу. IP-адреса могут быть статистическими и динамическими. Размещение в Сети информации, доступ к ней, а также внутрисетевой обмен информацией осуществляется при участии специализированных организаций – поставщиков услуг (провайдеров) [3, с. 71].

Вообще анализ функционирования компьютерных сетей позволяет прийти к выводу о том, что вся их система создавалась с таким расчетом, что в любое время существует возможность контролировать процесс перемещения информации внутри ее, а также установление источников ее происхождения и конечных потребителей. Это обстоятельство, с одной стороны, негативно отражается на соблюдении законных прав и интересов гражданина, с другой стороны, при соблюдении правовых аспектов, контроль сети позволяет эффективно выявлять, раскрывать и расследовать преступления, совершаемые в сфере оборота компьютерной информации.

Однако, по мнению ряда ученых, есть и определенные проблемы, существующие в процессе функционирования сети, которые негативно влияют на раскрытие и расследование рассматриваемых преступлений, характерные для нашего государства. Так, например, «Спамеры», как правило, используют электронные адреса вне домен-

ной зоны RU (Россия), что не позволяет своевременно получить сведения о нахождении их IP-адресов. Отсюда возникают две проблемы, одна из которых состоит в том, что потерпевший обращается в отдел полиции по месту жительства, где и должна производиться проверка сообщения о преступлении, но участники преступления проживают в других городах, следы преступления минимальны. Кроме сведений из компьютера потерпевшего (его компьютерной переписки) собрать какие-либо данные не представляется [9, с. 171–179].

Рассматривая характерные особенности функционирования компьютерной сети, можно сделать выводы о том, что с одной стороны, местом совершения мошенничества в сфере компьютерной информации является сама информационно-телекоммуникационная сеть, в которой происходит ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации. С другой стороны, местом совершения мошенничества в сфере компьютерной информации является местонахождение конкретного компьютера, с которого осуществляется неправомерный доступ. Надо отметить, что именно в этом месте находится основной объем информации, характеризующий процесс совершение преступления (способ, орудия и средства и т.п.), т.е. его следы.

Между тем, компьютерное мошенничество предусматривает наличие еще, как минимум одного, или нескольких устройств, которые будут вовлечены в процесс обменом информацией в целях извлечения сведений. При этом между такими устройствами может быть достаточно большое реальное расстояние. Приходится констатировать, что такое положение негативно сказывается на процессе выявления, раскрытия и расследования мошенничества в сфере компьютерной информации, особенно в тех случаях, когда неправомерный доступ к информации осуществляется из-за рубежа.

Таким образом, в рассматриваемом преступном деянии местом совершения преступления является местонахождение компьютерно-технических средств, с которого отправляются команды. Однако это не окончательное определение места совершения мошенничества в сфере компьютерной информации. Специфика установления признаков рассматриваемого преступного деяния обусловлена его двойственным объектом.

«Преступное деяние, – как отмечает в этой связи Н.А. Колоколов, – считается законченным с момента получения виновным суммы

денег (чужого имущества), а равно приобретения им юридического права на распоряжение такими деньгами (имуществом). Сам по себе факт ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей в зависимости от обстоятельств дела может содержать признаки приготовления к мошенничеству в сфере компьютерной информации или покушения на совершение такого преступления» [5, с. 6–15].

Таким образом, определение места совершения мошенничества в сфере компьютерной информации при установлении обстоятельств, подлежащих доказыванию, обладает определенной особенностью и влияет на формирование криминалистических знаний о данного вида преступлениях. Такая особенность обусловливает возможность использования знания о нем в процессе расследования. При этом кроме телекоммуникационной сети, местом совершения мошенничества являются места «обналичивания» денежных средств, полученных путем обмана. В зависимости от приемов и способов совершения мошенничества таковыми могут являться банкоматы, магазины, операционные залы банков и т.п.

Конечно, наиболее значимым для формирования криминалистического знания о мошенничестве в сфере компьютерной информации является то место, где находятся компьютерно-технические средства потерпевшего. Обусловлено это, как спецификой самой преступной деятельности мошенников, так и характером функционирования системы в которой она реализуется.

К таким, в частности относят: «сеть Интернет» – это международная информационно-телекоммуникационная сеть ЭВМ, не имеющая единого центра управления и организации, доступ к которой осуществляется посредством соединения по сети передачи данных (сеанса связи) [4].

Однако только одной сетью Интернет система обмена информацией не ограничивается. Это обстоятельство, по результатам проведенного исследования, позитивно влияет на процесс расследования рассматриваемого вида мошенничества. В частности, речь идет о киберпространстве. По мнению отдельных ученых «в состав «кибернетического пространства», входят [6, с. 15–16]:

– отдельные помещения или их набор, в которых размещены автоматизированные информационно-вычислительные системы с соот-

ветствующим техническим комплексом обеспечения ее деятельности (системы связи, электропитания, заземления и т.п.);

– средства автоматизированной обработки информации (вычислительные машины и их системы);

– каналы телекоммуникаций и передачи данных (в том числе звуковые волны и электромагнитные поля);

– машинные носители информации, обеспечивающие хранение информации в виде пригодном для ее автоматизированной обработки;

– непосредственно сама информация, представленная в виде пригодном для ее автоматизированной обработки (данные в соответствующих форматах, управляющие программы и т.п.);

– принятые порядок и последовательность (протоколы – по терминологии теории автоматизированных информационно вычислительных систем) автоматизированной обработки информации, а также установленные правила и распределение обязанностей между должностными лицами автоматизированной информационной системы».

Не вступая в полемику о необходимости отнесения того или иного элемента к кибернетическому пространству, отметим, что каждый из указанных элементов несет информативную составляющую, имеющую значение для формирования криминалистического знания о мошенничестве в сфере компьютерной информации и, как следствие расследования рассматриваемого вида преступлений.

Таким образом, наибольший интерес для формирования криминалистического знания о мошенничестве в сфере компьютерной информации и его расследования, представляют компьютерно-технические средства лица, на которое оказывалось преступное воздействие. Надо отметить, что в данном случае нас интересует именно компьютер потерпевшего, как источник информации и следов преступного воздействия. Такая особенность обусловлена тем, что существует определенная зависимость места совершения компьютерного мошенничества, с техническими средствами которыми оно совершается. Если, например, в месте нахождения лица, осуществляющего неправомерный доступ к компьютерной информации, в целях мошенничества, можно обнаружить весь спектр следов подозреваемого (следы пальцев рук на клавиатуре и других объектах, запаховые следы, иные выделения человека и т.п.), то в месте нахождения потерпевшего только его компьютерно-технические средства.

Список использованной литературы

1. Белкин Р.С. Криминалистическая энциклопедия. М. : Мегатрон XXI, 2000. 334 с.

2. Видонов Л.Г. Криминалистическая характеристика убийств и системы типовых версий о лицах, совершивших убийства без очевидцев. Горький : Прокуратура Горьк. обл., 1978. 122 с.

3. Воробец И.Н. Глобальная сеть Интернет как пространство для совершения преступлений // Доклады международной научно-практической конференции «Экономические, правовые и прикладные аспекты преодоления кризиса в европейских странах и России» / под ред. д.ю.н., проф. А.М. Кустова д.э.н., доц. Т.Ю. Прокофьевой. М., 2012. С. 71.

4. Илюшин Д.А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет : автореф. дис. … канд. юрид. наук. Волгоград. 2008. 22 с.

5. Колоколов Н.А. Преступления против собственности: комментируем новеллы УК РФ // Мировой судья. 2013. № 1. С. 6–15.

6. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации : автореф. дис. … д-ра юрид. наук. Воронеж, 2001. 39 с.

7. Смирнова И.Г, Коломинов В.В. Тактические особенности производства допроса по делам о преступлениях в сфере компьютерной информации [Электронный ресурс] // Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права). 2015. Т. 6. № 3. Режим доступа: http://eizvestia.isea.ru/reader/article.aspx?id=20140 (дата обращения: 17.09.2015).

8. Строгович М.С. Курс советского уголовного процесса. М. : Наука, 1968. Т. 1. 468 с.

9. Танасчишин А.А., Климчук Ю.А. Об опыте расследования уголовных дел по фактам мошенничества с использованием компьютерных технологий сети «Интернет», совершенных организованной группой // ИБ СД МВД России. 2013. № 1 (155). С. 171–179.

Информация об авторах

Коломинов Вячеслав Валентинович – преподаватель кафедры криминалистики и судебных экспертиз, Байкальский государствен-

ный университет экономики и права, 664003, г. Иркутск, ул. Ленина, д. 11, e-mail: OffRoad88@mail.ru.

Information about the author

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.

УДК 17(075.8)

С.В. Корнакова
О.С. Сергеева

О НЕКОТОРЫХ ПРОБЛЕМНЫХ АСПЕКТАХ ЭТИКИ ПРЕПОДАВАТЕЛЯ ВЫСШЕГО УЧЕБНОГО ЗАВЕДЕНИЯ

В статье затрагиваются некоторые этические проблемы профессиональной деятельности преподавателя высшей школы. Обращается внимание на взаимосвязь этической культуры преподавателя и качества преподавания. Делается вывод о важности обладания преподавателем не только глубокими научными познаниями, связанными с преподаваемым им курсом, но и высокими моральными качествами.

Ключевые слова: этика профессиональной деятельности, преподаватель высшей школы, культура общения.

S.V. Kornakova
S.O. Sergeeva

SOME OF THE PROBLEMATIC ASPECTS OF THE ETHICS OF EACHER OF HIGHER EDUCATIONAL INSTITUTION

The article touches on some ethical problems of professional activity of teacher of higher school. Attention is drawn to the interrelation between ethical culture of the teacher and quality of teaching. The conclusion about the importance of having a teacher not only deep scientific knowledge related to teaching their course, but also high moral character.