УГОЛОВНОЕ ПРАВО И УГОЛОВНЫЙ ПРОЦЕСС

УДК 343.98

АКТУАЛЬНЫЕ ПРОБЛЕМЫ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

И.О. Антонов, А.Н. Шалимов

Аннотация

В статье проанализированы особенности формирования криминалистической методики расследования мошенничества с использованием компьютерной информации. Обосновывается мнение о том, что эффективность расследования данной разновидности мошенничества во многом зависит от качества взаимодействия государственных правоохранительных органов между собой, а также с негосударственными структурами, выполняющими задачу по противодействию преступности в сфере телекоммуникаций и компьютерной информации. Выявление актуальных проблем, связанных с организацией эффективного противодействия мошенничеству с использованием компьютерной информации, позволит оптимизировать меры, направленные на профилактику данной разновидности мошенничества.

Ключевые слова: мошенничество, компьютерная информация, мошенничество с использованием компьютерной информации, расследование, методика расследования преступлений, преступления в сфере телекоммуникаций и компьютерной информации.

Компьютерные технологии, принеся бесспорную пользу для всего человечества, в то же время создали предпосылки для новых проявлений криминальной активности. Среди подобного рода явлений заметное место занимают всевозможные мошенничества.

По оценкам специалистов, двенадцать человек в мире ежесекундно становятся пострадавшими от действий киберпреступников (I). По некоторым данным, в Российской Федерации доходы киберпреступников исчисляются миллиардами долларов и наша страна постоянно входит в первую тройку стран-лидеров по числу киберугроз, число которых с каждым годом возрастает, а изощрённость удивляет (II). Немаловажным показателем для мошенничества с использованием компьютерной информации является количество вредоносных программ, которые обнаруживаются специалистами за сутки. Согласно статистике, ежедневно выявляется порядка 20 тысяч вредоносных программ, из них примерно 10% абсолютно новые (III).

Приведённые статистические данные, характеризующие состояние борьбы с киберпреступностью в целом и кибермошенничеством в частности, показывают, насколько злободневной является для отечественных правоохранительных органов задача по повышению эффективности борьбы с рассматриваемой категорией преступлений. При всём многообразии проблем, с которыми сталкиваются правоохранительные органы при расследовании кибермошенничества, в рамках статьи имеет смысл остановиться на анализе тех, которые, по нашему мнению, являются ключевыми.

Повышение эффективности предварительного расследования по уголовным делам о кибермошенничестве невозможно без определения факторов, которые способны оказывать заметное негативное влияние на качество процедуры расследования уголовного дела. Во-первых, это касается несовершенства норм отечественного уголовного права, предусматривающих ответственность за кибермошенничество. Данная проблема предопределяет неизбежное возникновение у правоприменителя сложностей в грамотной квалификации рассматриваемой разновидности мошенничества. Во-вторых, отсутствует в полной мере адекватное сложившейся криминогенной ситуации криминалистическое обеспечение процедуры расследования этой категории уголовных дел (как на уровне криминалистической методики, так и на уровнях криминалистической тактики и техники). В-третьих, степень профессиональной квалификации субъектов расследования не всегда в полной мере соответствует современным требованиям, что, безусловно, не может не сказаться на качестве предварительного расследования по уголовным делам о кибермошенничестве. В-четвёртых, негативное воздействие оказывает недостаточная координация совместных усилий правоохранительных органов с государственными и негосударственными структурами, специализирующимися на обеспечении безопасности в сфере телекоммуникаций и компьютерной информации.

Если оценивать состояние и тенденции развития отечественного уголовного законодательства, призванного стать основой борьбы с киберпреступностью, то важно отметить, что злободневность и сложность проблемы противодействия криминальной активности в сфере использования компьютерных технологий во многом предопределила направления и динамику совершенствования уголовного законодательства Российской Федерации последнего времени.

В этой связи в целом как позитивные можно оценить изменения, произошедшие в Уголовном кодексе РФ (далее – УК РФ) в 2011–2012 гг. В частности, одним из таковых можно считать введение в ст. 272 УК РФ понятия *компьютерная информация* (IV). Раскрытие законодателем содержания данного термина оказало положительное влияние на процедуру доказывания по уголовным делам, где можно обнаружить подобного рода информацию в качестве составляющей способа преступления. Кроме того, в указанный период законодателем была реализована идея расширения и детализации составов киберпреступлений. Так, в самостоятельную статью УК РФ (ст. 159.6) была выделена такая разновидность киберпреступности, как мошенничество в сфере компьютерной информации, что также оказало позитивное воздействие на практику противодействия кибермошенничеству. Как продолжение выбранной законодателем линии адаптации уголовного законодательства к реалиям сегодняшнего дня можно

рассматривать внесённый в Государственную думу Правительством России законопроект, призванный усилить ответственность за преступления в банковской сфере, совершаемые в целях хищения денежных средств с использованием высоких технологий (V).

Тем не менее трудно оспорить высказанные в литературе мнения, согласно которым вышеназванные изменения в отечественном законодательстве нельзя признать достаточными и во всём удачными (см., например, [1]). В частности, непродуманность ряда последствий выделения некоторых разновидностей мошенничества в самостоятельные составы уже не раз была предметом весьма критичного обсуждения специалистов (см., например, VI). Можно считать весьма точной оценку, согласно которой отдельные аспекты эффективности уголовно-правовых норм, регламентирующих ответственность за совершение преступлений в сфере компьютерной информации, обладают существенными недостатками, что отрицательно сказывается на результативности противодействия киберпреступности [2, с. 13].

В интересах эффективного доказывания по уголовным делам о кибермошенничестве необходимо продолжение работы законодателя по совершенствованию норм уголовного и уголовно-процессуального права в данном направлении. Перспективными можно признать предложения, в соответствии с которыми в УК РФ необходимо ввести категорию *компьютерная технология* и раскрыть её содержание для правоприменителя [3, с. 10]. Для достижения приемлемого уровня результативности в борьбе с киберпреступлениями необходимо создание адекватной существующим и потенциальным вызовам трансграничной правовой базы в этой сфере, так как современные инфокоммуникативные технологии делают весьма условными границы между государствами (VII).

Обозначенные изменения в отечественном законодательстве (произошедшие и ожидаемые) призваны повысить эффективность деятельности органов предварительного расследования по выявлению и расследованию кибермошенничеств. Появление новой самостоятельной статьи в УК РФ, предусматривающей наказание за мошенничество с использованием компьютерной информации, с долей оптимизма позволяет предположить, что правоохранительные органы получили в своё распоряжение более эффективный, чем ранее созданные, уголовно-правовой инструмент, ориентированный на одну из разновидностей мошенничества. Он призван обеспечить приемлемое качество процедуры выявления и расследования уголовных дел данной категории, а также неотвратимость изобличения и привлечения к уголовной ответственности лиц, виновных в совершении подобного рода киберпреступлений.

Введение законодателем в УК РФ ст. 159.6 предполагает целевую разработку и совершенствование соответствующего правового, организационного и методического обеспечения деятельности субъекта расследования по рассматриваемой категории уголовных дел. Иными словами, в современной криминалистической науке формирование частных криминалистических методик предопределяется вскрытием новых способов криминальных деяний и, соответственно, формированием в результате адекватного реагирования законодателя на сложившуюся ситуацию новых составов преступлений в уголовном законодательстве [4, с. 327].

Криминалистическая методика расследования мошенничества с использованием компьютерной информации изначально предполагает рациональное сочетание положений классической методики расследования мошенничества и ряда узловых положений методик расследования преступлений в сфере компьютерной информации. Важным структурным элементом криминалистической методики расследования мошенничества с использованием компьютерной информации является криминалистическая характеристика данной разновидности мошенничества. В ней, в свою очередь, ключевое место занимают способы подготовки, совершения и сокрытия данного преступления. Обладание информацией о способе мошенничества позволяет оптимизировать процесс выдвижения версии о других элементах предмета доказывания по уголовному делу этой категории.

В криминалистическом смысле способ мошенничества с использованием компьютерной информации имеет смысл обозначить как определённую криминальным замыслом систему действий по подготовке, совершению и сокрытию хищения чужого имущества или приобретения права на него посредством ввода, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Способы данной разновидности криминального обмана можно классифицировать по различным основаниям. На мошенничество с использованием компьютерной информации могут быть спроецированы уже известные классификации как мошенничества в целом, так и преступлений в сфере компьютерной информации.

Основой отделения данной разновидности мошенничества от других стало обязательное использование при совершении обмана различных манипуляций с компьютерной информацией (ввод, блокирование, модификация, иное вмешательство). Следовательно, предполагается, что тот, кто использует такого рода манипуляции для криминального обогащения, должен быть в большей или меньшей степени осведомлён о том, что представляют собой эти манипуляции, и, соответственно, обладать определённой квалификацией в сфере телекоммуникаций и компьютерной информации, достаточной для реализации криминального умысла.

Способ мошенничества с использованием компьютерной информации также предполагает применение аппаратно-программных средств, благодаря которым становится возможным криминальное вмешательство в штатное функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Не случайно, когда речь идёт о привлечении к уголовной ответственности мошенников рассматриваемой специализации, правоприменитель нередко квалифицирует криминальное деяние не только по ст. 159.6 УК РФ, но и по статьям о других преступлениях в сфере компьютерной информации, предусмотренных УК РФ (например, ст. 272 «Неправомерный доступ к компьютерной информации»). В частности, *Х*. был признан виновным за совершение преступлений, которые квалифицировались по ст. 159.6 и ст. 272 УК РФ (VIII). Девятнадцать эпизодов криминальной деятельности *Г*. были квалифицированы по ч. 3 ст. 272 и ч. 3 ст. 159.6 (IX).

Формы воздействия на компьютерную информацию, будучи обязательной составной частью данного вида мошенничества, предопределяют специфику следовой картины по указанному виду криминального обмана.

С точки зрения решения задач расследования важным является ранжирование способов мошенничества с использованием компьютерной информации в зависимости от характеристик лица либо лиц, совершивших хищение данного вида. Подобного рода мошенничества могут быть совершены с использованием служебного положения, то есть лицом, имеющим легальный доступ к компьютерной информации, в отношении которой осуществлено криминальное воздействие. Например, *Г.* совершил мошенничество в сфере компьютерной информации, используя свой служебный статус (старший бухгалтер) (Х).

Сложность деятельности по расследованию мошенничеств с использованием компьютерной информации возрастает пропорционально в зависимости от того, совершено ли криминальное деяние мошенником-одиночкой, организованной преступной группой или лицами, входящими в состав организованного преступного сообщества. Для организованных преступных групп и организованных преступных сообществ мошенничество с использованием компьютерной информации может быть лишь одним из направлений криминальной деятельности, причём оно может быть как основным, так и в какой-то мере второстепенным – обеспечивающим возможность совершения других преступлений. В организованных преступных группах мошенники нередко имеют криминальную специализацию (например, в группу могут входить те, кто непосредственно оказывает криминальное воздействие на компьютерную информацию с целью совершения хищения или приобретения прав на чужое имущество; а также те, кто решает иные задачи, не связанные с воздействием на компьютерную информацию).

Как у специалистов, так и у обывателей мошенничество с использованием компьютерной информации справедливо ассоциируется с транснациональной организованной киберпреступностью. Отнесение данного мошенничества к разновидности транснациональной преступности позволяет адекватно судить о его масштабности и латентности, а также о вероятности серьёзного противодействия расследованию подобного рода уголовных дел. Следовательно, эффективность процедуры их расследования во многом определяется результативностью взаимодействия отечественных правоохранительных органов с международными правоохранительными органами, правоохранительными органами зарубежных стран и рядом зарубежных негосударственных организаций, специализирующихся на оказании противодействия киберпреступности.

При отлаженности такого взаимодействия вероятность успешного расследования многих уголовных дел серьёзно повышается. Показательным в этом отношении является изобличение в совершении мошенничества, а также неправомерного доступа к компьютерной информации, использовании и распространении вредоносных программ братьев *П.* Признаётся, что успех расследования был обусловлен эффективным межведомственным взаимодействием следственных и оперативно-розыскных подразделений МВД и ФСБ России (Следственный департамент МВД России, Оперативное управление ЦИБ ФСБ России, УФСБ России по г. Санкт-Петербургу и Ленинградской, а также Калининградской областей,

БСТМ ГУ МВД России по г. Москве), участием в нём высококвалифицированных специалистов ЗАО «Лаборатория Касперского» (XI).

Для формирования эффективной криминалистической методики расследования мошенничества с использованием компьютерной информации трудно переоценить значение тактического обеспечения производства следственных действий и оперативно-розыскных мероприятий по данной категории уголовных дел. Особенности способа совершения рассматриваемой разновидности мошенничества предполагают и определённое своеобразие следовой картины, что, в свою очередь, ориентирует на разработку тактических средств, позволяющих оптимально задействовать технологии обнаружения и использования в доказывании следов мошенничества, совершённого с использованием компьютерной информации.

Успех расследования мошенничеств с использованием компьютерной информации во многом предопределяется количеством и качеством оперативно-розыскной информации, полученной ещё до возбуждения уголовного дела. Субъекту расследования крайне желательно, учитывая специфику противоправного воздействия на компьютерную информацию при совершении мошенничества, иметь в своём распоряжении уже на этапе, предшествующем возбуждению уголовного дела, максимально возможный объём сведений по основным позициям предмета доказывания. Такой информационный задел, с одной стороны, позволяет минимизировать риски по построению мошенниками результативной системы противодействия расследованию, а с другой – выполняет в случае необходимости своеобразную разъясняющую функцию для субъекта расследования, поскольку многообразие способов мошенничества с использованием компьютерной информации создаёт сложности в понимании технологических особенностей воздействия на компьютерную информацию при совершении такого рода преступлений.

Высокотехнологичность способов мошенничества с использованием компьютерной информации предопределяет немаловажную роль специалистов и экспертов при расследовании дел данной категории. Они способны оказать неоценимую помощь субъекту расследования как при подготовке, так и при производстве следственных действий. Нередко именно производство экспертиз создаёт успешные предпосылки для изобличения мошенников в совершении преступлений. Например, признаётся, что широкая экспертная поддержка специалистами антивирусной компании «Доктор Веб» обеспечила успех в расследовании одного из уголовных дел о мошенничестве, неправомерном доступе к компьютерной информации, создании, использовании и распространении вредоносных программ (XII).

Качество расследования мошенничества с использованием компьютерной информации (как и любого другого расследования) во многом определяется характеристиками проводящего его субъекта. Для того чтобы субъект расследования выполнял свои профессиональные обязанности на приемлемом уровне, он как минимум должен уверенно ориентироваться в сфере телекоммуникаций и компьютерной информации (прежде всего в тех её составляющих, где наиболее вероятно проявление криминальной активности мошенников), грамотно использовать имеющиеся в его распоряжении ресурсы для выявления следов воздействия

на компьютерную информацию с целью совершения мошеннических действий. Всё это возможно только при наличии определённого уровня профессиональной подготовки у субъекта расследования и реализации принципа специализации при расследовании рассматриваемой категории уголовных дел. В последнее время отмечаются позитивные изменения в данной области, в том числе успехи в становлении специализированных подразделений по борьбе с преступлениями в сфере информационных технологий (XIII).

В этой связи представляются весьма интересными высказанные в литературе суждения о том, что компьютерные технологии уже сами по себе предполагают особую логику в их применении, которая основана на строгой дисциплине, предъявляемой к процессу мышления. По этой причине преступления, для совершения которых используются данные технологии, являются в большинстве своём достаточно сложными. Безошибочной логике преступника должна противостоять безукоризненная логика следователя и лиц, содействующих ему в расследовании. Высокому интеллекту преступника должен противостоять не меньший, а по возможности больший интеллект сотрудников правоохранительных органов. Важным требованием к такому сотруднику является дисциплинированность, предполагающая способность к самоорганизации и сосредоточенности при решении непростых задач [5, с. 117].

В заключение необходимо отметить, что анализ актуальных проблем расследования мошенничества с использованием компьютерной информации имеет конечной целью совершенствование криминалистической методики в отношении данной разновидности криминального обмана. Качество криминалистической методики расследования мошенничества с использованием компьютерной информации во многом предопределяет эффективное решение задач предварительного расследования по уголовным делам рассматриваемой категории. Знание насущных проблем, связанных с организацией эффективного противодействия мошенничеству с использованием компьютерной информации, может быть востребовано при разработке мер, направленных на профилактику данной разновидности мошенничества.

Summary

I.O. Antonov, A.N. Shalimov. Urgent Problems in Investigation of Fraud Committed by Using Computer Information.

The main characteristics in the development of methods used for forensic investigation of fraud committed by using computer information are analyzed in the paper. It is substantiated that the efficiency of investigation of this type of fraud depends largely on the quality of interaction between various state law-enforcement bodies themselves and with non-state structures that are specified for preventing crimes in the sphere of telecommunications and computer information. Identification of current problems associated with the organization of counteraction to fraud committed by using computer information will favor optimization of measures aimed at preventing this type of fraud.

Keywords: fraud, computer information, fraud committed by using computer information, investigation, forensic techniques, crimes in the sphere of telecommunications and computer information.

Источники

I – По оценкам экспертов ежесекундно жертвами киберпреступников становятся 12 человек в мире // Пресс-служба Управления «К» МВД России. – URL: http://mvd.ru/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii/Publikacii_i_vistuplenija/item/1951798, свободный.

II – *Тросникова Д.* Российские киберпреступники заработали в 2013 году почти $2,5 млрд // Ведомости. – 2014. – 15 окт. – № 3696. – URL: http://www.vedomosti.ru/technology/articles/2014/10/15/dohody-hakerov-snizhayutsya, свободный.

III – *Захарова Я.* Заслон виртуальным мошенникам // MKRU. Краснодар. – 2012. – 10 апр. – URL: http://kuban.mk.ru/articles/2012/04/10/691501-zaslon-virtualnyim-moshennikam.html, свободный.

IV – Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (с изм. и доп.). – URL: http://www.consultant.ru/document/cons_doc_LAW_10699/, свободный.

V – Законопроект об усилении ответственности за хищения с помощью карт прошёл первое чтение в Госдуме // Ведомости. – 2014. – 19 нояб. – URL: http://www.vedomosti.ru/politics/news/2014/11/19/zakonoproekt-ob-usilenii-otvetstvennosti-za-hischeniya-s, свободный.

VI – *Берсенева Т.* Госдума хочет продолжить опыты над правоприменением // Право.ru. – 2013. – 23 мая. – URL: http://pravo.ru/review/view/85308/, свободный.

VII – *Лебедев П.* Российские суды снисходительны к киберпреступникам // CNews. – URL: http://www.cnews.ru/reviews/new/sredstva_zashchity_informatsii_i_biznesa_2013/articles/rossijskie_sudy_snishoditelny_k_kiberprestupnikam/, свободный.

VIII – Приговор от 22 февр. 2013 г. по уголовному делу № 1-121/2013 Кировского районного суда г. Уфы. – URL: http://kirovsky.bkr.sudrf.ru/modules.php?name=sud_delo&name_op=doc&srv_num, свободный.

IX – Приговор от 10 июня 2014 г. по уголовному делу № 1-141/2014 Октябрьского районного суда г. Самары. – URL: http://docs.pravo.ru/document/view/62001004/71225704/?line_id=7, свободный.

X – Приговор от 15 мая 2014 г. по уголовному делу № 1-49/2014 Хамовнического районного суда г. Москвы. – URL: http://docs.pravo.ru/document/view/63802454/74605806/?line_id=4, свободный.

XI – Вынесен приговор по первому в России уголовному делу о компьютерном «фишинге» // МВД России. – URL: http://mvd.ru/news/item/147552/, свободный.

XII – Сотрудникам Управления «К» МВД России удалось ликвидировать несколько крупнейших известных бот-сетей, построенных на основе «банковских троянов» // МВД России. – URL: http://mvd.ru/news/item/151919/, свободный.

XIII – В Иркутске Владимир Колокольцев провёл заседание объединённой коллегии министерств внутренних дел Союзного государства России и Белоруссии // МВД России. – URL: http://mvd.ru/document/1053381, свободный.

Литература

1. *Гладких В.И.* Компьютерное мошенничество: а были ли основания для криминализации? // Рос. следователь. – 2014. – № 22. – С. 25–31.

2. *Гарбатович Д.А.* Проблемные аспекты эффективности норм, предусматривающих ответственность за совершение преступлений в сфере компьютерной информации // Библиотека криминалиста. – 2013. – № 5. – С. 6–14.

3. *Сафонов О.М.* Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: Автореф. дис. … канд. юрид. наук. – М., 2015. – 22 с.

4. *Россинская Е.Р.* Криминалистика. – М.: Норма: ИНФРА-М, 2012. – 463 с.

5. *Подольный Н.А.* Отдельные проблемы расследования преступлений, совершённых с применением компьютерных технологий // Библиотека криминалиста. – 2013. – № 5. – С. 116–127.

Поступила в редакцию
08.05.15

Антонов Игорь Олегович – кандидат юридических наук, доцент кафедры уголовного процесса и криминалистики, Казанский (Приволжский) федеральный университет, г. Казань, Россия.

E-mail: *igolant@mail.ru*

Шалимов Анатолий Николаевич – кандидат юридических наук, доцент кафедры уголовного процесса и криминалистики, Казанский (Приволжский) федеральный университет, г. Казань, Россия.

E-mail: *an.shalimov@mail.ru*