УДК 343.37

И.А. Никитина

ФИНАНСОВОЕ МОШЕННИЧЕСТВО В СЕТИ ИНТЕРНЕТ

Рассматривается современное состояние финансового мошенничества в сети Интернет, анализируются преступные схемы, направленные на хищение чужих финансовых средств. Отмечается необходимость межгосударственного взаимодействия в борьбе с сетевой преступностью. Анализируются характерные признаки Интернет-мошенничества, информационно-технологические средства сети Интернет, которые используются преступниками для совершения хищений. Выделяются этапы осуществления мошеннических схем. Отмечается, что разнообразные мошеннические схемы в сети Интернет вызывают необходимость как национального, так и международного законодательного обеспечения борьбы с этим преступлением.
Ключевые слова: мошенничество; Интернет; преступные схемы.

Активное вовлечение России в мировое информационное пространство в начале 1990-х гг. дало мощный толчок развитию коммуникационных технологий, формированию глобальных компьютерных сетей, росту индустрии аппаратного и программного обеспечения, компьютеризации всех сфер экономики и повседневной жизни практически каждого человека.

Однако экономическая глобализация и интеграция отдельных государств в единую мировую систему несет в себе как положительный потенциал развития, так и ряд отрицательных факторов. Одним из них, способным негативно влиять на социальную жизнедеятельность, выступает преступность. В современных условиях она превращается в глобальную общечеловеческую проблему [1. С. 91]. Происходит интеллектуализация экономической преступности, которая использует новейшие достижения научно-технического прогресса в своих интересах. Интернет все более активно используется для незаконного проникновения в корпоративные и личные базы данных, совершения самых разнообразных мошеннических действий.

Компьютерные сети все шире применяются во многих областях жизни российского общества. Столь же быстро растет число преступлений, связанных с использованием сетевого доступа, множатся способы и формы совершения такого рода деяний. Отчетливо проявляется и тенденция возрастания размера наносимого ими ущерба.

По оценкам специалистов МВД, каждый год через Всемирную паутину российские преступники похищают со счетов фирм около 450 млн долл. [2. С. 7].

Количество преступлений, совершаемых в киберпространстве, растет пропорционально числу пользователей компьютерных сетей, и, по оценкам Интерпола, темпы роста преступности в глобальной сети Интернет являются самыми быстрыми на планете [3].

Интернет-мошенничество, по нашему мнению, является современной разновидностью традиционного мошенничества и представляет собой хищение чужого имущества либо приобретение права на чужое имущество путем обмана или злоупотребления доверием, совершенное с использованием сети Интернет.

Этот вид мошенничества имеет две составляющие: психологическую и технологическую [4]. Психологическая составляющая воздействует на значимые элементы мотивации потенциальной жертвы и побуждает ее к совершению действий в интересах мошенников. Такими элементами воздействия могут быть:

1) стремление к получению прибыли. Быстрое обогащение – основа большинства мошеннических предложений (например, инвестиционное мошенничество, финансовые пирамиды);

2) желание бесплатно получить некоторые платные услуги и товары (например, предложения неоплачиваемой сотовой связи и доступа в Интернет);

3) стремление к приобретению отдельных предметов, которые либо затруднительно, либо невозможно приобрести другими путями. Это способствует различному виду аукционного мошенничества и продажам несуществующих товаров и услуг;

4) отзывчивость и жалость.

На основе этих элементов человеческой психики мошенники строят различные схемы попрошайничества (мнимый сбор средств для детского дома, на помощь неизлечимо больным, пострадавшим от катастроф и т.д.).

Технологическая составляющая дает современному мошеннику возможность, во-первых, донести необходимую информацию до потенциальной жертвы; во-вторых, обеспечить свою анонимность и безопасность; в-третьих, получить от жертвы деньги, не вступая с ней в непосредственный контакт.

Мошенники в ходе проведения своих афер могут использовать следующие информационно-технические средства сети Интернет:

1. World Wide Web, или «всемирная паутина», – огромная составляющая сети Интернет, объединяющая миллионы веб-сайтов.

2. E-mail – электронная почта – популярная интернет-служба, которой пользуются миллионы жителей планеты, активно используется мошенниками для рассылки спама (массовой рассылки электронных сообщений без согласия их адресатов) и проведения фитинговых операций [5. С. 38–40].

3. BBS – система электронных досок объявлений, наиболее популярная в США и менее популярная среди отечественных пользователей.

4. Электронные платежные системы и виртуальные деньги. Особой привлекательностью среди российских мошенников пользуются такие системы, как Яндекс-деньги, Web-money.

Указанные средства не являются неизменными, т.к. технологии развиваются и в сети постоянно появляются новые возможности, которыми могут воспользоваться мошенники.

Важное значение имеют не только информационно-технологические возможности, но и те особенности, благодаря которым стало реальным их использование в качестве средств совершения преступления. К ним можно отнести следующие:

– отсутствие постоянного и эффективного контроля за достоверностью представляемой информации, за корректностью сведений, рассылаемых по электронной

почте и размещаемых объявлений на электронных досках и веб-сайтах;

– отсутствие действенной системы обмена информацией о жалобах пользователей сети Интернет;

– отсутствие механизма исполнения гражданско-правовых обязательств в сети Интернет.

Являясь принципиально новым явлением, интернет-мошенничество имеет характерные признаки, которые выделяют его из всей массы преступных деяний. К ним можно отнести следующие:

– высокая степень латентности;

– многообразие способов совершения преступлений;

– транснациональный, глобальный характер деятельности;

– сложности и особенности в уголовно-процессуальном производстве, преимущественно на стадии досудебного рассмотрения, в том числе касающиеся сбора доказательств.

Потерпевшими от интернет-мошенничества могут быть как физические, так и юридические лица. В большинстве случаев в качестве основных потерпевших выступают юридические лица, т.к. в ходе аннулирования платежных операций убытки несут именно они.

Сеть Интернет, при наличии определенных знаний и навыков, обеспечивает большую степень анонимности для мошенников. Эти обстоятельства свидетельствуют о том, что интернет-мошенничество – это один из самых латентных видов преступлений, противостоять которому наше информационное общество оказалось не готово.

Все многообразие мошеннических схем с использованием Интернета можно разделить на следующие группы: онлайн-аукционы; доставка товаров; партнерские программы; предложения несуществующих товаров и услуг; «нигерийские письма», «черные невесты», мошенничество с использованием технологий сотовой связи; фишинг.

В сети Интернет в настоящее время широко распространен мошеннический обман в намерениях, когда виновный обманывает потерпевшего относительно своих действительных намерений. Такой обман налицо в случаях, когда виновный получает от потерпевшего деньги, обещая оказать определенную услугу, выполнить работу (например, организовать подключение к сети Интернет), берет имущество в долг при получении кредита и т.п., хотя фактически не имеет намерения ни выполнять работу или услугу, ни возвращать вещь, ни погашать долг.

Получение путем обмана услуг или работ, неисполнение обязательств имущественного характера, передача должного мошенничеством не являются, поскольку не связаны ни с хищением чужого имущества, ни с приобретением прав на чужое имущество. В соответствующих случаях подобные действия могут рассматриваться как причинение имущественного ущерба путем обмана или злоупотребления доверием и квалифицироваться по ст. 165 УК РФ.

Мошенничество путем злоупотребления доверием налицо, если виновный использует для хищения имущества доверительное отношение владельца имущества. Например, использует реквизиты доверенной ему платежной банковской карты для покупок товара в интернет-магазинах. В последнее время, в связи с развитием в России глобальных компьютерных сетей, появилась возможность получения информации при помощи несанкционированного доступа в локальные сети (например, банковских, страховых компаний и т.д.). Мошенники активно используют различного рода вредоносные программы (трояны, сетевые черви), помогающие осуществить незаконный доступ к информации.

В соответствии с п. 12 Постановления Пленума Верховного Суда РФ от 27 декабря 2007 г. № 51 как мошенничество квалифицируется безвозмездное обращение лицом в свою пользу или в пользу других лиц денежных средств, находящихся на счетах в банках, совершенное с корыстной целью путем обмана или злоупотребления доверием. В случаях, когда указанные деяния сопряжены с неправомерным внедрением в чужую информационную систему или с иным неправомерным доступом к охраняемой законом компьютерной информации кредитных учреждений либо с созданием заведомо вредоносных программ для ЭВМ, внесением изменений в существующие программы, использованием или распространением вредоносных программ для ЭВМ, содеянное подлежит квалификации по ст. 159 УК РФ, а также, в зависимости от обстоятельств дела, по ст. 272 или 273 УК РФ, если в результате неправомерного доступа к компьютерной информации произошло уничтожение, блокировки, модификация либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети [6].

Другим вариантом мошеннических действий, связанных с использованием сети Интернет, может служить использование созданного по подложным документам лжепредприятия, вступившего на договорной основе в платежную систему. Это облегчает авторизацию поддельных карт, реквизиты которых могут быть получены самыми разными способами (при помощи несанкционированного доступа в сети и др.). Перечисленные на счет лжепредприятия с этих карт денежные средства в дальнейшем по платежному поручению перечисляются на счета других предприятий, также созданных по подложным документам, а затем изымаются. Действия по осуществлению мошеннических схем в сети Интернет условно можно разделить на три этапа:

1. Передача информации потенциальной жертве с целью введения ее в заблуждение.

2. Непосредственное завладение предметом посягательства.

3. Временной период между завладением предметом посягательства и пониманием жертвой того, что ее обманули. Этот временной промежуток может составлять от нескольких недель до 1 года [7. С. 169].

Наиболее распространенными способами передачи информации являются веб-сайты и электронная почта. Веб-сайт, как правило, регистрируется на бесплатном хостинге, чтобы соблюсти анонимность. Однако возможно и то, что мошенники размещают сайт на серверах достаточно респектабельных хостинг-компаний.

Непосредственное завладение предметом посягательства осуществляется после того, как жертва введена в заблуждение и готова выполнить предлагаемые ей условия, например осуществить предоплату. Возможны две формы завладения предметом посягательства: ввод регистрационных данных кредитных карт и пере-

вод «электронной наличности». Первая форма, как правило, присутствует при фишинге, где основной целью фишеров являются именно «креды» – регистрационные данные кредитных карт. Перевод электронных денег (Web-money, Яндекс-деньги) наиболее характерен для схем с предоплатой (сотовое мошенничество, предложение несуществующих товаров). Этот этап также характеризуется тем, что обманутые все еще верят мошенникам и даже не догадываются, что стали жертвой мошенничества.

На последнем этапе жертва понимает то, что ее обманули. Для таких комбинаций, как предложение несуществующих товаров и услуг, данный этап, как правило, длится не более 1 месяца. Когда речь идет о фишинге, то здесь сроки могут быть самыми разными. Все зависит от бдительности самого потерпевшего. В любом случае, когда фишинг обнаруживается, потерпевший всегда может опротестовать «свои» расходы, и конечным потерпевшим, как правило, остается интернет-магазин либо иное юридическое лицо, услугами которого воспользовались фишеры.

В отличие от традиционного мошенничества, характерной чертой интернет-мошенничества является то, что оно, как правило, оставляет мало следов преступления и потерпевшие не знают преступников в лицо. При этом крайне сложно выявить и идентифицировать личность мошенника.

Интернет, став крупнейшим международным каналом обмена информации, практически стер все социальные, психологические и возрастные границы. В Интернете часто нельзя быть полностью уверенным, что человек, с которым вы общаетесь, именно тот, за кого он себя выдает. Специалисты также отмечают, что среди интернет-мошенников все чаще проявляется тенденция к «омоложению».

В последнее время среди интернет-мошенников наблюдается стремление к консолидации своих преступных усилий. Так создаются преступные группы и целые преступные транснациональные сообщества [8].

Разнообразные мошеннические схемы в сети Интернет вызывают необходимость как национального, так и международного законодательного обеспечения борьбы с этим преступлением.

Интернет-мошенничество – труднодоказуемое преступление. Сложности обусловлены различными факторами. Наиболее значимыми являются те, которые вытекают из особенностей самой сети Интернет. Отсутствие законодательного регулирования сети Интернет или пробелы в нем в различных странах мира, несогласованность межгосударственного взаимодействия в борьбе с сетевой преступностью делают Интернет притягательным для мошенников. В последние годы предпринимаются настойчивые и масштабные попытки стран объединить усилия в борьбе с мошенничеством в сети Интернет.

Анализ активно развивающихся схем мошенничества в Интернете позволяет высказать следующие предложения, направленные на предотвращение, выявление растущих угроз развитию сети Интернет:

– необходимо использовать положительный аспект создания специализированных центров сбора и анализа информации о случаях мошенничества в сети Интернет;

– необходимо изучение международного законодательства с целью выработки единых понятий и скоординированных мероприятий по борьбе с интернет-мошенничеством;

– транснациональный характер интернет-мошенничества требует практической согласованности действий правоохранительных систем различных стран, и прежде всего, тех, организации и население которых в наибольшей степени страдают от последствий подобных преступлений;

– учитывая быстрое развитие информационных технологий, необходимо ставить перед разработчиками программного обеспечения, производителями оборудования, службами, занимающимися информационной безопасностью, и другими структурами вопросы о предотвращении возможностей для мошеннических действий.

Важной задачей государственных органов, в том числе и правоохранительных, является информационно-просветительская деятельность об угрозе со стороны мошенников, действующих в сети Интернет.

Эти меры профилактического характера помогут сузить сферы преступных посягательств и позволят выявить многие из них на ранней стадии.

ЛИТЕРАТУРА

1. *Багаутдинов Ф.Н., Хафизова Л.С.* Финансовое мошенничество (уголовно-правовой и криминологический аспекты противодействия). М.: Юрлитинформ, 2008. 280 с.
2. *Осипенко А.Л.* Борьба с преступностью в глобальных компьютерных сетях: Международный опыт. М., 2004. 432 с.
3. *Номоконов В.А.* Глобализация информационных процессов и преступность. URL: http:www.crime-reseach.org/library/nomohon.htm
4. *Хренов С.* Интернет-мошенничество с использованием технологий сотовой связи. URL: http://www.breru/security/13296/html
5. *Альтовский Е.* Правовое противодействие спаму // Информационное право. 2006. № 3. С. 38–40.
6. *Постановление* Пленума Верховного Суда РФ от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате».
7. *Криминалистическая* методика расследования отдельных видов преступлений: Учеб.: В 2 ч. / Под ред. А.П. Резвана, М.В. Субботиной. М., 2002. 371 с.
8. *В Испании* задержаны российские Интернет-мошенники. URL: http://www.crimerescarch.ru/news/14.05.2004/234/

Статья представлена научной редакцией «Право» 1 июня 2010 г.