УДК 343

Н.В. Олиндер*

О КРИМИНАЛИСТИЧЕСКОЙ КЛАССИФИКАЦИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СРЕДСТВ И СИСТЕМ

В статье предложена авторская классификация преступлений, совершенных с использованием электронных платежных средств и систем, по следующим признакам: по объекту преступного посягательства; по предмету преступного посягательства; в зависимости от субъектов преступления – по количеству субъектов; по признаку территориальности; по способу совершения.

Ключевые слова: преступления, современные с использованием электронных платежных средств и систем, криминалистическая классификация преступлений.

Множественность преступлений, совершенных с использованием электронных платежных систем и средств, дает возможность их криминалистической классификации. С использованием электронных платежных средств и систем могут быть совершены следующие виды преступлений: различного рода интернет-мошенничества, интернет-кражи, вымогательство, легализация доходов, полученных незаконным путем, интернет-казино, взяточничество, незаконное предпринимательство, компьютерные преступления. В работах некоторых авторов можно встретить еще дополнительные виды преступлений: незаконные получение и разглашение сведений, составляющих коммерческую или банковскую тайну; изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов [1].

Нам представляется целесообразным выделение нескольких оснований криминалистической классификации преступлений, совершенных с использованием электронных платежных средств и систем.

1. По объекту преступного посягательства.

1.1. Преступления против собственности (мошенничество, кража, вымогательство).

1.1.1. Мошенничество, совершенное с использованием электронных платежных систем и средств.

В числе наиболее распространенных способов совершения мошенничества с электронными платежными средствами значатся фишинг, финансовые пирамиды, онлайн-аукционы и иные действия, связанные с обманом или злоупотреблением доверием, при совершении которых на некотором этапе преступления используются электронные платежные средства, в результате чего похищается чужое имущество или приобретается право на него. Следует подчеркнуть, что в глобальной сети Интернет уже развиты почти все виды мошенничества, которые существуют в реальной жизни.

Некоторыми распространенными схемами мошенничества, совершаемого с использованием электронных платежных систем и средств, на данный момент являются: создание «инвест-фондов», на сайтах которых пользователю предлагается сделать денеж-

---

*Олиндер Нина Владимировна (*v@yandex.ru*)*, кафедра уголовного процесса и криминалистики, Самарский государственный университет, 443110, Российская Федерация, г. Самара, ул. Акад. Павлова, 1.

ный вклад под проценты; продажа украденной бытовой техники; требование внести деньги за регистрацию в фирме, предлагающей высокий заработок при работе на дому. Также существуют десятки других схем мошенничества, жертвами которых зачастую становятся даже опытные пользователи сети [2].

Вместе с тем следует отметить, что виды мошенничества, совершаемого с использованием электронных платежных систем и средств, могут быть выявлены в результате анализа заявлений от потерпевших, которые поступают в Центр по расследованию интернет-мошенничеств Internet Fraud Complaint Center (IFCC). Все преступления данного вида могут быть разбиты на следующие основные группы:

– мошеннические действия при проведении интернет-аукционов (68 % заявлений);

– недопоставка товаров, которые были оплачены в интернет-магазинах (22 %); – мошенничество с номерами кредитных карт (5 %);

– банковские махинации, инвестиционные виды мошенничества и разные схемы многоуровневого сетевого маркетинга (5 %)[3].

1.1.2. Кража, совершенная с использованием электронных платежных систем и средств.

Основным способом совершения кражи с использованием электронных платежных систем и средств является неправомерное получение и использование чужих учетных данных (логинов и паролей) для доступа к чужому электронному кошельку. Такие учетные данные могут быть получены посредством вредоносных программ, запускаемых на компьютере клиента электронной платежной системы, на котором установлена отдельная программа для доступа к электронному кошельку, либо если клиент осуществляет такой доступ через WEB-интерфейс платежной системы.

Дополнительными способами совершения краж с использованием электронных платежных систем и средств являются: атака на сервер оператора платежной системы при помощи вредоносных программ; атака при помощи вредоносных программ на канал связи между сетевым оборудованием клиента и сетью оператора платежной системы [4].

В настоящее время растет число выявленных и раскрытых преступлений рассматриваемой категории. Например, в 2009 году была пресечена деятельность преступной группы, члены которой с помощью вредоносной программы, разработанной одним из участников группы, получили неправомерный доступ к счетам корпоративных клиентов Объединённой системы моментальных платежей (ОСМП), похитили их денежные средства (по доказанным эпизодам сумма составила 5,6 млн руб.), после чего отмывали такие денежные средства путем многократного перевода их в титульные знаки различных электронных платежных систем, при этом кроме электронных кошельков использовались и счета клиентов различных операторов мобильной связи [5].

1.1.3. Вымогательство.

Уголовное законодательство определяет вымогательство как требование передачи чужого имущества или права на имущество или совершение других действий имущественного характера под угрозой применения насилия либо уничтожения или повреждения чужого имущества, а равно под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких. Принимая во внимание, что криминальная среда все больше проникает в сферу высоких технологий, в том числе в информационно-телекоммуникационную среду, и учитывая реалии бизнеса в информационной сфере, констатируем, что появились новые виды преступлений общеуголовного характера, но уже с использованием при их совершении компьютерных технологий. Наиболее распространенным способом совершения таких преступлений сегодня являются так называемые DDoS-атаки.

Вымогательство в данном случае связано с выдвижением предварительных требований вымогателей к владельцу сервера, интернет-портала, сайта о выплате некоторой суммы под угрозой DDoS-атаки. Выплаты за непроведение DDoS-атаки всегда проводятся на предоставленный вымогателями электронный кошелек любой из электронных платежных систем, оформленный на вымышленное лицо.

В 2010 году разоблачена и обезврежена преступная группа, занимавшаяся вымогательством подобного рода. Преступники, используя глобальную сеть Интернет и вредоносные программы, получали управление над большим количеством компьютеров (так называемые ботнет-сети) и в последующем осуществляли атаки на компьютеры своих жертв, полностью блокируя их работу, с последующим требованием денег за прекращение атаки. Для перечисления денег преступники предлагали электронные кошельки в различных платежных системах, преимущественно Webmoney, затем деньги обналичивались в различных городах России и стран СНГ. В результате проведенных оперативно-розыскных мероприятий преступники были выявлены. Ими оказались жители Москвы, Новосибирска и Иркутской области, которые дистанционно управляли созданной ими сетью. Установлено, что преступниками было атаковано более 50 информационных ресурсов различных организаций [6].

1.2. Преступления в сфере экономической деятельности (незаконное предпринимательство, легализация доходов, полученных незаконным путем).

1.2.1. Легализация доходов, полученных незаконным путем, с использованием электронных платежных средств и систем.

В отношении данного вида преступлений подробный анализ проведен Е.Л. Логиновым [7]. Автор отмечает, что легализация и отмывание денег, полученных незаконным путем, в половине случаев проходит именно через электронные платежные системы. Осуществление расчетов и переводов денежных средств в этих системах достаточно просто с технической стороны: можно зарегистрировать несколько кошельков и зачислять на них незаконно полученные средства с целью дальнейшего обналичивания. В кредитных организациях проводится четкий контроль в сфере отмывания денег (например, при приеме денежных средств от физических лиц на квитанции указываются паспортные данные и ставится подпись), в электронных платежных системах такие платежи отследить крайне трудно. Помимо этого, электронные платежные средства можно обменивать между различными платежными системами и переводить с одного кошелька в другой, контроль за такими операциями не осуществляется, что повышает интерес преступников к таким действиям.

1.2.2. Незаконное предпринимательство.

В данной группе могут быть выделены преступления, связанные с незаконной деятельностью интернет-казино, букмекерских контор (тотализаторов), лотерей и аукционов. Данный вид преступлений в настоящее время не может быть отнесен к мошенничеству, так как установлен прямой запрет на осуществление такой деятельности, поэтому логичнее отнести их к незаконному предпринимательству.

В настоящее время в криминальной практике существуют два основных способа проведения интернет-лотереи. Первый используют недобросовестные законно действующие интернет-магазины. Они объявляют на своих сайтах, что начинается розыгрыш какого-либо товара, пользующегося повышенным покупательским спросом и, соответственно, дорогого. Чтобы принять участие в этой «лотерее», необходимо сначала купить в этом интернет-магазине какой-либо сопутствующий, как правило, не пользующийся спросом товар, например два компакт-диска. После получения купленного товара якобы розыгрыш будет происходить только среди его покупателей. Однако впоследствии розыгрыш ожидаемого товара не проводится, хотя на сайте интернет-магазина появляется соответствующая информация о его проведении.

Во втором случае преступники регистрируют платный номер мобильного телефона, счет которого «привязан» к электронному кошельку в некоторой платежной системе, оформленному на вымышленное лицо, после чего от имени некоторой фирмы объявляют «электронный тотализатор», в ходе которого предлагают отправить sms-сообщения на этот платный номер. В качестве приза участнику, отправившему большее количество sms-сообщений или каждое 1000-е сообщение, предлагается автомобиль, туристическая путевка на двоих или иной потенциально ценный выигрыш.

Можно отметить, что в данной группе электронные платежные средства и системы будут выступать и в качестве предмета преступного посягательства, и как средство совершения преступления.

1.3. Преступления в сфере компьютерной информации.

В данной группе выделяют деяния, приводящие к уничтожению, блокированию, модификации либо копированию охраняемой законом информации, нарушению работы ЭВМ, системы ЭВМ или их сети, и осуществляемые либо посредством неправомерного доступа к компьютерной информации (ст. 272 УК РФ), либо посредством вредоносных программ для ЭВМ (ст. 273 УК РФ), либо при нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ). Практически все преступления, совершенные с использованием электронных платежных средств и систем, содержат «компонент» преступлений, предусмотренных главой 28 УК РФ: при их осуществлении преступник может получить неправомерный доступ к компьютерной информации, использовать вредоносные программы, нарушать правила эксплуатации ЭВМ, системы ЭВМ или их сети.

В связи со спецификой рассматриваемых преступлений в данной классификационной группе выделим два структурных элемента.

1.3.1. Неправомерный доступ к компьютерной информации, являющейся информационным объектом электронных платежных систем.

По данному составу можно квалифицировать преступления, которые нацелены на неправомерный доступ к логинам, паролям и ключам виртуального кошелька и платежной системы в целом, если владелец электронной платежной системы предпринял меры по отнесению такой информации к охраняемой законом – например, ввел режим коммерческой тайны либо объявил такую информацию служебной тайной.

1.3.2. Создание, использование и распространение вредоносных программ для ЭВМ, предназначенных для осуществления неправомерных действий в электронных платежных системах или с электронными платежными средствами.

Изученные нами материалы уголовных дел и открытые публикации позволяют сделать вывод о том, что у разработчиков вредоносных программ существует специализация, связанная с разработкой программ для неправомерных действий преимущественно в электронных платежных системах или с электронными платежными средствами. К таким программам относятся: Clampi, Zeus, другие программы. Для оперативного информирования о новых разработках, получения справочной информации о технологии работы систем электронных платежей, необходимой для создания новых или модификации имеющихся программ, существуют специализированные форумы (например, ZloY TEaM ForuM, размещенный по адресу https://forum.zloy.bz), на которых имеются также темы, касающиеся продаж информации, полученной при помощи вредоносных программ и содержащей реквизиты доступа пользователей к счетам в электронных платежных системах.

1.4. Преступления против государственной власти, интересов государственной службы и службы в органах местного самоуправления (дача взятки посредством электронных платежных средств и систем; получение взятки посредством электронных платежных средств и систем).

Взятка с использованием электронных платежных систем и средств сопряжена с передачей взяточнику не наличных денег, а реквизитов доступа к электронному кошельку, в котором находятся титульные знаки, имеющие денежный эквивалент. Доказать в этом случае факт получения взятки весьма затруднительно.

Таким образом, в классификации, где квалификационным признаком будет выступать закрепление в нормах Уголовного кодекса РФ, нами выделено четыре группы преступлений, совершенных с использованием электронных платежных средств и систем.

2. По предмету преступного посягательства преступления, совершенные с использованием электронных платежных средств и систем, можно подразделить на две группы:

2.1. Преступления, имеющие материальный предмет посягательства.

К таковым, по нашему мнению, необходимо отнести преступления, направленные на хищение денежных средств и совершенные посредством электронной платежной системы. Однако причиненным ущерб будет считаться только в том случае, если произошло обналичивание денежных средств и потерпевшему причинен реальный ущерб. До момента перевода электронных платежных средств данные знаки являются электронными средствами учета.

2.2. Преступления, не имеющие материального предмета посягательства.

К ним необходимо отнести преступления, объектом которых является охраняемая законом компьютерная информация.

На примере предмета хищения можно выделить три признака предмета преступного посягательства: материальный (визуальный, выражается в наличии вещи); экономический (предмет преступного посягательства обладает стоимостью); юридический (всегда присутствует собственник). В рассматриваемых нами преступлениях достаточно часто будет отсутствовать материальный признак предмета преступного посягательства.

3. В зависимости от субъектов преступления – по количеству субъектов (преступления, совершенные одним лицом, преступления, совершенные группой лиц).

Чаще всего преступления рассматриваемой категории совершаются группой лиц, в которой каждый из членов группы специализируется на определенных операциях, например, создании вредоносной программы для похищения реквизитов доступа к электронной платежной системе и сбыт этой программы; покупке и использовании вредоносной программы для создания массива похищенных у пользователей реквизитов доступа к электронной платежной системе, сбыте такого информационного массива; покупке информационного массива с реквизитами доступа и осуществлении хищения титульных знаков, перевода их на иные электронные кошельки, возможно, в иных электронных платежных системах, продаже титульных знаков ниже номинала; обналичивании денежных средств.

4. По признаку территориальности – предмет преступления, субъект преступления, потерпевший находятся на территории одного государства; наличествует один из вариантов размещения предмета преступления, субъекта преступления, потерпевшего на территории разных государств.

Данный классификационный признак имеет большое значение, так как существенно детерминирует специфику расследования рассматриваемого вида преступлений. Связано это с особенностями подготовки, совершения преступления, особенностью следственных действий и т. д.

Рассматриваемые преступления всегда совершаются с помощью удаленного доступа, что отличает их от преступлений, совершенных иным способом. Например, кража, совершенная традиционным способом, предполагает обязательное нахождение преступника на расстоянии физической доступности от похищаемого имущества, вследствие чего преступник должен проникнуть в некоторое помещение или приблизиться к некоторому субъекту, обеспечить скрытность своих действий.

При совершении кражи посредством электронной платежной системы преступник может находиться сколь угодно далеко от потерпевшего и от похищаемых денежных средств, поскольку для совершения преступления использует удаленный доступ. При этом преступник с использованием собственной компьютерной техники первоначально удаленно взаимодействует с компьютером потерпевшего, на котором хранятся учетные данные для авторизации в электронной платежной системе, и/или с сервером, на котором хранится иная информация о платежах клиента электронной платежной системы. В зависимости от того, на территории одного или разных государств находятся потерпевший и субъект преступления, последнему приходится учитывать при подготовке и совершении преступления такие факторы, как различие часовых поясов, языковых и иных настроек операционной системы и прикладных программ, функционирующих на компьютере преступника и его жертвы, особенности антивирусной защиты атакуемого компьютера, технологическую специфику электронной платежной системы, иные факторы.

5. По способу совершения.

5.1. Использование уязвимости электронной платежной системы без неправомерного использования реквизитов доступа ее легального пользователя. Поскольку электронная платежная система является сложной аппаратно-программной системой, включающей различные подсистемы и каналы передачи данных, то ее элементы имеют технологические особенности, позволяющие неправомерно использовать их при подготовке и совершении преступления. Такие выявленные специалистами особенности называются уязвимостями, а процесс их использования в неправомерных действиях – эксплуатацией, использованием уязвимостей.

Например, осенью 2010 года появились сообщения о выявленной уязвимости в электронной платежной системе Perfect Money, позволяющей обмануть систему, предоставив ложные данные об оплате заказа. В течение некоторого времени, пока уязвимость не была устранена, любой злоумышленник мог имитировать перевод денег за товар или услугу в системе Perfect Money, при этом заплатив всего 10 центов. В качестве потерпевших могли выступить интернет-магазины, которые потенциально могли получить от системы Perfect Money уведомление о том, что тот или иной счет, выставленный ими, был оплачен полностью. Увидеть, что фактически средств на счету недостаточно, продавец мог только после проверки своего баланса [8].

5.2. Неправомерное использование реквизитов доступа легального пользователя электронной платежной системы. Данный способ совершения преступления является самым распространенным и фактически традиционным вследствие того, что клиенты электронных платежных систем уделяют недостаточное внимание проблеме обеспечения сохранности собственных реквизитов доступа к платежной системе. Заражение компьютера вредоносными программами, скрытно собирающими конфиденциальную информацию, включая такие реквизиты, происходит на этапе подготовки преступления. В дальнейшем эти реквизиты вместе с реквизитами, похищенными у других клиентов электронной платежной системы, объединяются в массивы, которые продаются другим участникам преступной группы, обеспечивающим так называемый вывод денег из платежной системы на этапе совершения преступления.

Приведенная классификация не исключает и не ограничивает дополнительное исследование преступлений, совершенных с использованием электронных платежных средств и систем, может быть детализирована и дополнена.

Библиографический список

1. Джафарли В.Ф. Уголовная ответственность за совершение хищений в банковской сфере, связанных с использованием электронных платежных средств: дис. ... канд. юрид. наук : 12.00.08. М., 2003. 168 с. РГБ ОД, 61:04-12/264-9.

2. Куда сообщить о мошенничестве в Интернете? [Электронный ресурс]. URL: http://veslohotron.ucoz.ru/index/0-9.
3. Титунина Е. Мошенничество в сфере функционирования электронных платежных систем – проблемы противодействия [Электронный ресурс]. URL: http://www.crime-research.ru/articles/titunina1207.
4. Павперов Е. Риски мошенничества в системах электронных платежей [Электронный ресурс]. URL: http://econcrime.ru/expert/3.
5. Хакеры, взломавшие ОСМП, ждут суда [Электронный ресурс]. URL: http://veq.ru/catalog/news-zakon/doc/525. Загл. с экр
6. Нургалиев Р.Г. Электронный патруль // Российская газета. 2010. 16 октября. 10 полоса
7. Логинов Е.Л. Отмывание денег через интернет-технологии: Методы использования электронных финансовых технологий для легализации криминальных доходов и уклонения от уплаты налогов: учеб. пособие для студентов вузов. М., 2005. С. 25–28.
8. Есть ли уязвимость в Perfect Money? [Электронный ресурс]. URL: http://webmoneyinfo.net/news/34-est-li-uyazvimost-v-perfect-money.html.

References

1. Dzhafarli V.F. *Ugolovnaia otvetstvennost' za sovershenie khishchenii v bankovskoi sfere, sviazannykh s ispol'zovaniem elektronnykh platezhnykh sredstv: dis. ... kand. iurid. nauk : 12.00.08* [Criminal responsibility for commission of embezzlement in banking sphere connected with the use of electronic means of payment: Candidate's of Law thesis: 12.00.08]. M., 2003, 168 p. Russian State Library Department of Doctorate, 61: 04–12/264-9 [in Russian]
2. Where to address in connection with Internet crime? Retrieved from: http://veslohotron.ucoz.ru/index/0-9 [in Russian]
3. Titunina E. Fraud in the sphere of functioning of electronic payment services – problems of countering. Retrieved from: http://www.crime-research.ru/articles/titunina1207 [in Russian]
4. Pavperov E. Risks of fraud in the electronic payment systems. Retrieved from: http://econcrime.ru/expert/3 [in Russian]
5. Hakers that broke OSMP system abide by the courts decision. Retrieved from: http://veq.ru/catalog/news-zakon/doc/525 [in Russian]
6. Nurgaliev R.G. Electronic patrol. Rossiiskaia Gazeta, 2010, 16 October. 10 page [in Russian]
7. Loginov E.L. Money laundering through Internet technologies: Methods of use of electronic financial technologies for the legalization of criminal revenues and evasion of taxes: textbook for the students of Institutions of Higher Education. M., 2005, pp. 25–28 [in Russian]
8. Is there a sensitivity in Perfect Money? Retrieved from: http://webmoneyinfo.net/news/34-est-li-uyazvimost-v-perfect-money.html. [in Russian]

N.V. Olinder*

ABOUT CRIMINALISTIC CLASSIFICATION OF CRIMES COMMITTED WITH THE USE OF ELECTRONIC PAYMENT FACILITIES AND SYSTEMS

The article offers the author's classification of crimes sovereshnno using electronic payment instruments and systems by the following features: a criminal assault on the facility; on the subject of a criminal assault; depending on the subjects of the crime – the number of subjects; on the basis of territoriality; by the process of committing.

Key words: crime, sovereshnno using electronic payment instruments and systems, forensic kalssifikatsiya crimes.

* *Olinder Nina Vladimirovna* (v@yandex.ru), Department of Criminal Procedure and Criminalistics, Samara State University, Samara, 443110, Russian Federation.

УДК 343.98

*О.А. Славгородская**

КРИМИНАЛИСТИЧЕСКОЕ ИЗУЧЕНИЕ ЛИЧНОСТИ СВИДЕТЕЛЯ В ДОКАЗЫВАНИИ ПО УГОЛОВНЫМ ДЕЛАМ

В статье проанализированы особенности процесса доказывания по уголовным делам с учетом соотношения и взаимосвязи криминалистики и уголовного процесса. Отмечается роль С.А. Шейфера в формировании доказательственного права. Рассматриваются особенности производства допроса свидетеля и анализируются закономерности, влияющие на качество получения доказательств, с учетом специфики и доказательственного значения указанного следственного действия. Обосновывается необходимость совершенствования уголовно-процессуальной деятельности и резюмируется востребованность разработки основ криминалистического изучения личности свидетеля.

Ключевые слова: доказывание, допрос, криминалистическое изучение, личность, показания, расследование, свидетель, теория.

Основой любого успешного расследования является процесс собирания, проверки и использования доказательств. Вопросы доказывания в процессе производства расследования по уголовным делам не только становятся предметом дискуссий среди теоретиков и практиков, но и способствуют появлению серьезных научных исследований.

Большой вклад в развитие теории доказательственного права внес профессор С.А. Шейфер. В его диссертационном исследовании на соискание ученой степени доктора юридических наук «**Методологические и правовые проблемы собирания доказательств в советском уголовном процессе» и таких работах, как:** «Собирание доказательств в советском уголовном процессе: Методологические и правовые проблемы», «Доказательства и доказывание по уголовным делам», были сформулированы основы современной теории судебных доказательств.

Подчеркивая ключевую роль доказывания как «сердцевины уголовного процесса», профессор С.А. Шейфер акцентирует внимание на том, что «получение доказательств и оперирование ими в целях воссоздания действительной картины изучаемого события является единственным средством достижения целей судопроизводства, т. е. защиты прав и законных интересов потерпевшего и ограждения личности от незаконного привлечения к уголовной ответственности, ограничения ее прав и свобод» [1, с. 16].

Совершенствование процесса доказывания в уголовном судопроизводстве служит связующим звеном для внедрения криминалистических рекомендаций и разработок в следственную и судебную практику в строгом соответствии с требованиями закона. Именно в данном направлении наиболее явно проявляется взаимодействие криминалистики и уголовно-процессуального права и определяется их прикладное значение.

Славгородская Ольга Александровна (slavkur-htc@yandex.ru), кафедра криминалистики, Саратовская государственная юридическая академия, 410056, г. Саратов, ул. Чернышевского, д. 104.