# Вопросы квалификации мошенничества в сфере компьютерной информации

**А.А. Энгельгардт**

доцент кафедры уголовного права и криминалистики факультета права Национального исследовательского университета «Высшая школа экономики», кандидат юридических наук. Адрес: 101000, Российская Федерация, Москва, Мясницкая ул., 20. E-mail: aengelgardt@hse.ru

**Аннотация**

Статья посвящена отдельным вопросам квалификации мошенничества в сфере компьютерной информации. Автор делает вывод, что эту сферу как объективный признак состава рассматриваемого преступления образуют те области, где практическую деятельность (фактические и юридические действия) составляет функционирование электронных платежных систем, в которых дистанционно совершаются операции с использованием банковских карт, безналичных денег и т.п. Не выходя за пределы этой сферы, виновный может приобрести противоправную имущественную выгоду (приобрести отношение к имуществу как к своему) в виде безналичных денег, бездокументарных ценных бумаг, иного права на имущество. Об этом свидетельствует приводимая в статье обширная судебная практика. Совершение хищения наличных денег, иных материальных предметов, как правило, «заставляет» на каком-то этапе исполнения операции в сфере компьютерной информации сочетать с действиями вне информационной среды: изготовлением поддельных доверенностей, обманным получением дубликатов сим-карт, изъятием наличных денежных средств и др. В условиях, когда уголовная ответственность за хищения дифференцируется в зависимости от его способов (форм), эти обстоятельства могут привести к конкуренции при правовой оценке содеянного. Предлагается исходить из следующих соображений. Новые запреты включаются в существующую, сложившуюся за долгие годы систему. Действия, которые всегда оценивались как кража или иное хищение, не могут поменять своей природы в связи с их выполнением в части указанным в ст. 159.6 УК РФ способом. Например, если посредством совершения операций в сфере компьютерной информации субъект еще не получил господства над объектом посягательства, и для получения возможности реально распоряжаться и пользоваться им он должен тайно изъять имущество, это будет уже кража. Таким образом, в круг деяний, квалифицируемых по статье 159.6 УК РФ, нужно ввести лишь те, когда для завершения преступления не требуется наряду с указанными в статье действиями в сфере компьютерной информации совершение иных действий, оцениваемых как способ изъятия (обособления или удержания) предмета, присущего иной форме хищения. Судебная практика пока не дает явных, да даже неявных оснований для выводов, что данный подход принят по существу.

**Ключевые слова**

уголовный запрет, общая и специальная нормы, преступление, уголовная ответственность, предмет преступления, компьютерная информация, мошенничество, толкование уголовно-правовых норм.

Библиографическое описание: Энгельгардт А.А. Вопросы квалификации мошенничества в сфере компьютерной информации // Право. Журнал Высшей школы экономики. 2016. № 4. С. 86–95.

JEL: K14; УДК: 343 DOI: 10.17323/2072-8166.2016.4.86.95

По природе вещей технологии создаются для того, чтобы приносить пользу, но ими нередко злоупотребляют. На то, что их развитие проявилось в новых способах хищения чужого имущества или приобретения права на чужое имущество, требуя в современных условиях со стороны государства установления адекватных уголовно-правовых мер, обращено внимание в Пояснительной записке к проекту федерального закона о внесении в Уголовный кодекс Российской Федерации (далее — УК РФ) дополнений и изменений, касающихся уголовной ответственности за мошенничество[1].

Так же, как преступления в сфере компьютерной информации (гл. 28 УК РФ), предусмотренное ст. 159.6 УК РФ деяние связано с описанными в законе нарушениями в области информационных и коммуникационных технологий, использующих компьютерную информацию. Состав установлен, но заслуживает отдельного исследования имеющая практически-правовое значение проблема должной определенности объективных признаков уголовно-правового предписания ст. 159.6 УК РФ[2]. Несмотря на казуистичный характер описания деяния, некоторые его характеристики, связанные с содержанием, границами проявления и др., представляют сложность для толкования и могут зависеть от точки зрения конкретного правоприменителя.

В частности, установленный ст. 159.6 УК РФ запрет связан с криминообразующим признаком совершения преступления «в сфере компьютерной информации». Что указывается этим признаком в данном случае? Если взглянуть на него с точки зрения теории состава преступления, по всей видимости, законодатель указывает на обстановку, в которой реализуются используемые при этом субъектом способы и средства совершения преступления. В пользу такой трактовки уголовного закона говорит системное прочтение ч. 5 ст. 159, ст. 159.1 и 159.5–159.6 УК РФ[3].

Сферу компьютерной информации как объективный признак состава рассматриваемого преступления при такой трактовке образуют те области, где практическую деятельность (фактические и юридические действия) составляет функционирование электронных платежных систем, в которых дистанционно совершаются операции с использованием банковских карт, безналичных денег и т.п. Для совершения данных операций без участия человека компьютерная информация может быть введена (установлена), иным образом обработана в электронной памяти не только компьютера, но и тех технических устройств, которые по своему характеру способны выполнять функции приема, переработки, хранения, передачи и выдачи информации в электронном виде (прим. 1 к ст. 272 УК РФ). К числу таких устройств могут относиться, например, смартфоны, мобильные телефоны, POS-терминалы, платежные терминалы (в том числе банкоматы, вендинговые аппараты), контрольно-кассовые машины. В имеющихся публи-

[1] Цит. по: Отзыв кафедры уголовного права юридического факультета МГУ им. М.В. Ломоносова о проекте федерального закона о внесении в УК РФ дополнений и изменений, касающихся уголовной ответственности за мошенничество // http://www.iuaj.net/node/1169( дата обращения: 4.10.2016). В дальнейшем, если в ссылке не приведены страницы использованного издания, ссылка сделана на электронные базы данных (КонсультантПлюс, Гарант).

[2] Определенность уголовного закона сформулирована А.Э. Жалинским как такое соответствие его текста воле законодателя, которое позволяет различным субъектам правоприменения, действуя в различных ситуациях, неоднократно: а) получать на основе толкования текста закона однородные описания этой воли; б) отделять установленные законодателем пределы судейского усмотрения от неясности и неопределенности предписаний закона и возможных нелегитимных произвольных правоприменительных решений. См.: *Жалинский А.Э.* Уголовно-экономическое право: проблематика определенности закона (российские и немецкие взгляды) / Избранные труды: в 4 т. Т. 2. М., 2015. С. 318.

[3] *Есаков Г.А.* Уголовный закон и предприниматели: достижения и просчеты / Уголовное право и современность: сборник научных статей. Вып. 5.М., 2014. С. 111.

кациях судебных приговоров по данной группе дел отсутствуют ссылки на какие-либо ограничения по их видам, хотя далеко не все из перечисленных устройств упомянуты.

Непосредственно из предшествующего изложения проистекает слабая сторона признака: указание на сферу компьютерной информации как область, где совершается преступное деяние, не показывает пределы действия комментируемой статьи так, чтобы это позволило надежно разграничить деяние со смежными преступлениями. Не пытаясь здесь решить все связанные с этим вопросы, попробуем высказать определенные рекомендации, обеспечивающие «перевод» теоретических положений в практически применяемый алгоритм правовой оценки совершенного преступления[4].

В большинстве случаев для разграничения мошенничества в сфере компьютерной информации с другими разновидностями хищений, как правило, достаточно опереться на отдельные выделенные в уголовном законе и (или) разработанные судебной практикой признаки как основания квалификации совершенного деяния. Например, в отличие от мошенничества, предусмотренного ст. 159–159.3,159.5 УК РФ, для анализируемого преступления не характерны: обман человека и передача имущества или приобретение права на имущество с помощью потерпевшего, вызываемые им имущественные последствия являются следствием воздействия виновного на компьютерную информацию как средство совершения преступления. Указанный признак позволяет обосновать применение общей нормы о мошенничестве — ст. 159 УК РФ — в ситуации, когда держатель платежной карты посредством ввода компьютерной информации в систему «банк-онлайн» снимает деньги со своего счета, а в банк посылает электронное уведомление о похищении у него (несанкционированном списании) денежных средств, чтобы получить компенсацию. Дальнейшие операции по проверке заявления, зачислению денежных средств на счет заявителя, в том числе в сфере компьютерной информации, совершают уполномоченные работники банка. Вследствие того, что имущественное распоряжение о компенсации совершает под влиянием обмана работник потерпевшего банка, квалифицировать ситуацию по ст. 159.6 УК РФ нельзя[5].

Значение других признаков, например, предмета совершаемого деяния, не столь очевидно. Компьютерные технологии в настоящее время включены во многие процессы, связанные со стоящими под защитой действующих правовых норм имущественными благами. Оставаясь в сфере компьютерной информации, можно обеспечить динамику (в частности, переход и подтверждение) вещных и обязательственных прав от одного субъекта к другому. Соответственно, при совершении мошенничества в сфере компьютерной информации и не выходя за пределы этой сферы, виновный может приобрести противоправную имущественную выгоду (приобрести отношение к имуществу как к своему) в виде безналичных денег, бездокументарных ценных бумаг, иного права на имущество. Так, при хищении безналичных денежных средств мошенничество в сфере компьютерной информации окончено с момента зачисления денег на банковский счет лица, поскольку оно получает реальную возможность распоряжаться поступившими в результате преступных действий денежными средствами по своему усмотрению. Например, осуществлять расчеты от своего имени или от имени третьих лиц, не обна-

[4] В статье рассматриваются лишь некоторые проблемы определенности объективных признаков уголовно-правового предписания статьи 159.6 УК РФ, и лишь в порядке постановки вопроса. В частности, не затрагиваются: характеристика ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации; правила квалификации компьютерного мошенничества и преступлений, предусмотренных главой 28 УК РФ, и др.

[5] *Третьяк М.* Проблемы квалификации новых способов мошенничества // Уголовное право. 2015. № 2. С. 94–98.

личивая денежных средств со счета, на который они были перечислены в результате мошенничества[6].

Продолжая разбираться с поставленным вопросом, можно заметить, что о возможном выражении предмета мошенничества в сфере компьютерной информации в виде безналичных денежных средств — права на чужое имущество — свидетельствует обширная судебная практика. По ст. 159.6 УК РФ квалифицируются действия, состоящие, в частности, в использовании:

- подложного (от имени владельца счета) электронного платежного поручения, направляемого через систему «Банк-Клиент». С объективной стороны это предполагает проникновение помимо санкции банка в его компьютерную систему, ввод и (или) модификацию циркулирующей в ней компьютерной информации, что влечет перечисление безналичных денежных средств на счет виновного или иной счет, средствами на котором он может воспользоваться как своими;
- программы дистанционного банковского обслуживания счета, примененной для несанкционированной модификации компьютерной информации. С помощью программы виновные направляют подложное платежное поручение о перечислении денег на те счета, средствами на которых они имеют реальную возможность распорядиться в пользу виновного или других лиц;
- вредоносной компьютерной программы, обеспечивающей замену файла платежного поручения, направленного посредством электронной системы «Банк-Клиент» владельцем денег на счете в банке на файл, содержащий подложное поручение и реквизиты счета, подконтрольного уже виновному;
- банковской карты организации, дающей возможность несанкционированного отдаленного доступа к управлению расчетным счетом организации и перечисления с данного счета путем вмешательства в функционирование банковских средств хранения, обработки или передачи компьютерной информации денежных средств (за исключением случая хищения их в наличной форме);
- фиктивных трудовых договоров, внесения на их основе подложных сведений в табели учета рабочего времени «мертвых душ», предоставления их в электронной форме в бухгалтерию с последующим перечислением заработной платы, начисленной на фиктивно трудоустроенных лиц, на подконтрольные виновному банковские счета;
- не заблокированной или ошибочно подключенной к номеру телефона услуги «Мобильный банк», оказываемой в сфере компьютерной информации и предоставляющей право распоряжаться денежными средствами, находящимися в ЭПС или на счете владельца телефонного номера;
- кредитных карт, оформленных через электронную программу «Кредитный брокер» на физических лиц, ранее приобретавших товары в кредит. Преступники используют их личные данные, сохранившиеся в системной памяти базы торговой организации. После активирования карт деньги обналичиваются через банкомат;
- полученных путем использования вредоносных программ логинов и паролей, с помощью которых владелец счета управлял движением безналичных денежных средств, для направления в банк через сеть Интернет распоряжения о перечислении средств на подконтрольные виновному счета в другом или том же банке;
- полученных по поддельной доверенности дубликата сим-карты номера сотового телефона гражданина и информации о его банковских счетах для несанкционированного входа в компьютерную программу удаленного доступа к счетам клиентов –«Банк

[6] Постановление Пленума Верховного Суда РФ от 27.12.2007 №51 «О судебной практике по делам о мошенничестве, присвоении и растрате» (п.12).

Онлайн» — и направления распоряжения о перечислении средств на подконтрольный виновному счет[7].

Во всех приведенных случаях предусмотренное ст. 159.6 УК РФ посягательство на чужое имущество, получение возможности распоряжаться им как своим собственным (свидетельствующее об окончании преступления) состоялось в форме приобретения права на чужое имущество. Обналичивание похищенных безналичных денежных средств находилось уже за пределами состава.

По позиции законодателя, выраженной в диспозиции ст. 159.6 УК РФ, предметом посягательства при компьютерном мошенничестве могут являться и вещи, например, деньги в наличной форме, электронные устройства. Позиция законодателя именно такова, а закон должен исполняться.

Подходы судебной практики к данному вопросу, несомненно, определяются позицией Пленума Верховного Суда РФ о квалификации хищения как кражи в случаях, если деяние связано с получением наличных денег из банкомата[8]. По-видимому, не нужно доказывать, что это датированное 2007 годом толкование выводилось из двух оснований: а) получение наличных денежных средств находится в пределах объективной стороны состава хищения, б) осуществляется без участия уполномоченного работника кредитной организации. Факт вмешательства при этом виновного в функционирование систем банкомата, являющихся средствами хранения и обработки компьютерной информации, в постановлении не оценивался.

После выделения в уголовном законе мошенничества в сфере компьютерной информации появились предложения о корректировке Верховным Судом РФ позиции по рассматриваемой ситуации в «пользу» нового состава, поскольку конституирующие признаки состава преступления, предусмотренного ст. 159.6 УК РФ, по своему содержанию соответствуют признакам ситуации. В этом плане показательно мнение М. Третьяк: «В связи с появлением специального состава мошенничества в сфере компьютерной информации хищение чужих денежных средств путем использования похищенной или поддельной расчетной карты, если выдача наличных денег осуществляется банкоматом, без участия в операции уполномоченного работника кредитной организации, необходимо квалифицировать не как кражу, а по статье 159.6 УК»[9]. Итак, во-первых, предложение определяется тем, что в данной норме отсутствует указание на факт воздействия непосредственно на интеллектуальную и волевую сферы собственника или иного потерпевшего посредством обмана, направленного на их побуждение к имущественному распоряжению — передаче имущества. Во-вторых, тем, что объективная сторона преступления предполагает действия в сфере компьютерной информации как причину

[7] *Добровольский В.И.* Мошенничество в сфере кредитования и смежные составы преступлений: вопросы применения и разграничения ст. 159.1, 159.3 УК и иных составов преступлений//СПС КонсультантПлюс. См. также: *Потапкин С.Н., Солдатов А.В., Утешева Т.Т., Данилов Д.А.* Вопросы объективной стороны мошенничества в сфере компьютерной информации в судебно-следственной практике//Библиотека научных публикаций электронного периодического справочника «Система Гарант» 2015. №1; *Тюнин В.* «Реструктуризация» уголовного законодательства об ответственности за мошенничество // Уголовное право. 2013. №2. С. 41.

[8] Постановление Пленума Верховного Суда РФ от 27.12.2007 №51 «О судебной практике по делам о мошенничестве, присвоении и растрате»(п.13). В литературе, впрочем, отмечаются отдельные примеры вменения при совершении виновным указанных действий мошенничества по статье 159 УК РФ. См.: Кассационное определение Московского городского суда от 1.08.2012 по делу №22-9940/2012. Цит. по: *Третьяк М.* Правила квалификации компьютерного мошенничества и преступлений, предусмотренных гл. 28 УК РФ // Уголовное право. 2014. № 4. С. 74.

[9] *Третьяк М.* Указ. соч. С. 74.

причинения ущерба собственнику или иному владельцу имущества. Ситуация связана с вмешательством в функционирование программного обеспечения банкомата.

Суды стали широко применять ст. 159.6 УК РФ, когда действия виновного, начатые в сфере компьютерной информации, завершаются последующим изъятием или присвоением материальных предметов. Так, по ст. 159.6 УК РФ были осуждены П. и Е., работавшие менеджерами офиса продаж. По предварительному сговору, используя служебный компьютер, они произвели в электронных товарных накладных модификацию данных — замену артикулов дорогостоящей продукции на артикулы менее дорогой продукции. Получив таким образом возможность скрыть от учета более дорогие товары, они похитили, как сказано в приговоре, товаров на сумму 344144 руб. из офиса продаж, и обратили в свое пользование[10].

Другой пример. Сотрудник компании сотовой связи N., зная о схеме, позволяющей путем ввода и модификации данных компьютерной программы «1С» оплачивать товары по сниженной стоимости, зашел под чужим именем в указанную программу, ввел наименование товара — смартфон марки «iPhone 4S», выбрал способ оплаты (кредитной картой), указав сумму оплаты 1 (один) рубль. Затем с помощью POS-терминала совершил в сфере компьютерной информации операцию, в результате которой с банковской карты был списан 1 рубль, а модуль оплаты отразил получение платы на полную стоимость смартфона, который N. похитил[11].

В литературе предлагаются и иные ситуации, когда деяние, связанное с получением в итоге наличных денежных средств, заслуживает квалификации по ст. 159.6 УК РФ. Например, руководитель организации после оформления фиктивных платежных документов посредством электронной платежной системы переведет денежные средства на расчетный счет другой организации, руководитель которой обналичит эти средства и передаст руководителю первой организации, оставив себе небольшое вознаграждение за «услугу»[12].

В приведенных случаях и примерах виновными использовался соответствующий способ действия — ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Признак совершения действий в сфере компьютерной информации стал определяющим фактором квалификации хищений по ст. 159.6 УК РФ. Обоснованность такого подхода как универсального вызывает сомнение. В частности:

- если на каком-то этапе исполнения деяния операции в сфере компьютерной информации сочетаются с действиями вне информационной среды: изготовлением поддельных доверенностей, обманным получением дубликатов сим-карти др.;
- этот аргумент кажется недостаточным и тогда, когда модификация компьютерной информации приводит к возможности получения виновным имущества в виде материальных предметов, а сама реализация указанной возможности (например, изъятие и (или) обращение наличных денежных средств в пользу виновного или других лиц) входит в объективную сторону деяния, как в известном примере с банкоматом.

В условиях, когда уголовная ответственность за хищения дифференцируется в зависимости от его способов (форм), эти обстоятельства могут привести к конкуренции при правовой оценке содеянного. Даже тщательная оценка всех обстоятельств отдель-

[10] Приговор Пресненского районного суда Москвы 2013 г. Уголовное дело №1-176/2013 / Судебные решения РФ // bsr/case/6511205 (дата обращения: 5.10.2016)

[11] Приговор Самарского районного суда Самары 2014 г. Уголовное дело №1-34/2014/Судебные решения РФ // gcourts.ru/case/23839448(дата обращения: 5.10.2016)

[12] *Потапкин С.Н., Солдатов А.В., Утешева Т.Т., Данилов Д.А.* Указ. соч. // СПС «Гарант».

ного случая не позволит разрешить ее с должной степенью определенности. Целесообразно все же сформулировать соображения общего порядка, обеспечивающее конвенциональное применение судами норм УК РФ. Основы работы со статьями главы 21 УК РФ, получения на их основе правовой оценки отдельных видов деяний могут меняться с изменением уголовного закона. Но новые запреты включаются в существующую, сложившуюся за долгие годы систему. Уголовно-правовая информация, циркулирующая в этой системе, надежно программирует практическую деятельность адресатов. Действия, которые всегда оценивались как кража или иное хищение, не могут поменять своей природы в связи с их совершением указанным в ст. 159.6 УК РФ способом. Поэтому, на наш взгляд, необходимо ограничение круга деяний, квалифицируемых по ст. 159.6 УК РФ, по следующим основаниям:

• проникновение (вход) в информационную среду, действия в сфере компьютерной информации могут быть совершены только для того, чтобы облегчить доступ к чужому имуществу, облегчить совершение и (или) сокрытия преступления. Тогда ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей не выступают в качестве способа хищения, и последнее не может квалифицироваться по ст. 159.6 УК РФ. В таких случаях в преступном деянии будет присутствовать какая-либо из иных форм хищения — например, кража, присвоение;

• посредством операций в сфере компьютерной информации (ее ввода, удаления, модификации, др.) субъект может еще не получить господства над объектом посягательства. Для получения возможности им распоряжаться и пользоваться он должен, в частности, либо: а) тайно изъять имущество. Это — уже кража; б) совершить действия, направленные на обращение вверенного имущества в свою пользу (например, скрыть наличие такого имущества у него путем подлога в электронных документах). Это будет присвоение.

Таким образом, в круг деяний, квалифицируемых по ст. 159.6 УК РФ, нужно ввести лишь те, когда для завершения преступления не требуется наряду с действиями в сфере компьютерной информации совершение иных действий, юридически оцениваемых как способ изъятия (обособления или удержания) предмета, присущего иной форме хищения. Судебная практика пока не дает явных, да даже неявных оснований для выводов, что данный подход принят по существу.

Как видно, масштабное изменение уголовного законодательства об ответственности за мошенничество, приведшее к появлению целого семейства специальных норм об ответственности за различные виды мошенничества, повлекло возникновение новых проблем. Любые попытки дать ответ на вопрос, стала ли уголовно-правовая защита имущественных отношений более совершенной с введением ответственности за мошенничество в сфере компьютерной информации, уже по определению являются спорными. В литературе высказываются многочисленные соображения о трудностях толкования ст. 159.6 УК РФ, о рисках снижения предсказуемости уголовно-правовых решений, возникающих в процессе применения ее предписаний. Вполне понятно желание их анализа и поиск способов преодоления связанных с ними трудностей на основе выработки надежной аргументации.

Следует продолжить исследование оснований идентичности рассматриваемого запрета как мошенничества в сфере компьютерной информации или как особого вида хищения, поскольку возникло устойчивое мнение, что новая норма «переросла» рамки ответственности за мошенничество. Различия между «старым» мошенничеством и мошенничеством в сфере компьютерной информации, вытекающие из присущих последнему особенностей, немалы. Эффективность реализации ст. 159.6 УК РФ о мошенничестве в сфере компьютерной информации в немалой степени зависит от понимания особенностей признаков объективной стороны состава, в частности, установленного в

статье специфического способа посягательства, как главного условия четкого разграничения указанных посягательств со смежными имущественными преступлениями.

Поскольку анализируемые законоположения уже реализуются, для исключения недопустимо резких поворотов практики, желательно их толкование в соответствующих практикообразующих документах.

## Библиография


Добровольский В.И. Мошенничество в сфере кредитования и смежные составы преступлений: вопросы применения и разграничения ст. 159.1, 159.3 УК и иных составов преступлений. 2014//СПС КонсультантПлюс

Есаков Г.А. Уголовный закон и предприниматели: достижения и просчеты / Уголовное право и современность: сборник научных статей. Вып. 5.М.: Проспект, 2014. С.104–122.

Жалинский А.Э. Уголовно-экономическое право: проблематика определенности закона (российские и немецкие взгляды) / Жалинский А.Э. Избранные труды: в 4 т. Т.2. М.: НИУ ВШЭ, 2015. С. 317–329.

Кочои С.М. Преступления против собственности: пособие для магистрантов. М.: Проспект, 2014. 88 с.

Лопашенко Н. А. Посягательства на собственность: монография. М.: Норма, 2012. 527 с.

Лопашенко Н.А. Законодательная реформа мошенничества: вынужденные вопросы и вынужденные ответы // Криминологический журнал Байкальского государственного университета экономики и права. Т. 9. 2015. №3. С. 504–513.

Потапкин С.Н., Солдатов А.В., Утешева Т.Т., Данилов Д.А. Вопросы объективной стороны мошенничества в сфере компьютерной информации в судебно-следственной практике // Библиотека научных публикаций электронного периодического справочника «Система Гарант» 2015. №1.

Смолин С. Уголовно-правовая борьба с высокотехнологичными способами и средствами совершения преступлений//Уголовное право. 2014. №4. С. 62–68.

Третьяк М. Мошенничество как преступление против собственности в современном уголовном праве: курс лекций. М.: Юрлитинформ, 2014. 200 с.

Третьяк М. Проблемы квалификации новых способов мошенничества // Уголовное право. 2015. № 2. С. 94–98.

Третьяк М. Правила квалификации компьютерного мошенничества и преступлений, предусмотренных гл. 28 УК РФ // Уголовное право. 2014. № 4. С.69–74.

Тюнин В. «Реструктуризация» уголовного законодательства об ответственности за мошенничество//Уголовное право. 2013. № 2. С.35–41.

Шумихин В.Г. Седьмая форма хищения чужого имущества//Вестник Пермского университета. Юридические науки. 2014. Вып. 2. С. 229–233.

Южин А.А. Мошенничество и его виды в российском уголовном праве: дис… канд. юрид. наук. М., 2016. 238 с.

Яни П.С. Специальные виды мошенничества. Статья шестая // Законность. 2015. №8. С. 35–40.


# The Issues of Classifying Fraud in the Computer Information Area


## Artur Engelgardt

Associate Professor, Department of Criminal Law and Criminalistics, Law Faculty, National Research University Higher School of Economics, Candidate of Juridical Sciences. Address: 20 Myasnitskaya Str., 101000, Moscow, Russian Federation. E-mail: aengelgardt@hse.ru

## Abstract

The article deals with the legal issues of classifying computer fraud. The author concludes that the area as a clear sign of cyber-fraud consists of the activity (physical and juridical acts) related to functioning electronic payment systems, e.g. distant financial operations involving bank cards, non-cash money etc. An offender may gain the illegal material profit (acquire illegal title to some property) in the form of bank money, book-entry securities, other property rights without going outside the bounds of the cyber-sphere. The author presents a great number of legal cases to support this thesis. At the same time, committing a theft of cash money or other material property usually requires to combining cyber-activity with some physical interactions. It may include preparation of fictitious warrants, taking out cash-money, etc. In the circumstances where the criminal liability depends on the form of illegal appropriation one can face a collision in legal treatment of criminal actions. The author draws the conclusion that there is a possibility to find out the solution to the problem. The new prohibitions of the Criminal Code should be included in the existing system of prescriptions. A theft should be treated as a theft even if it has been committed as defined in Art. 159.6 of the Criminal Code. For example, if a theft should be qualified actions of an offender who made some cyber-operations but did not get the possibility to control assessments, the thief has to make other physical actions to appropriate it. Consequently, Art. 159 of the Criminal Code covers only the actions in the cyberspace that are enough to acquire title to some property and do not require additional activity in order to appropriate (to hold back) these objects. The analysis of the court practice does not allow concluding that the law enforcer has similar views on the issue nowadays.



## Keywords

criminal prohibition, common and special norms, crime, criminal liability, target of crime, computer information, fraud, interpretation of criminal rules.

Citation: Engelgardt A.A. (2016) The Issues of Classifying Fraud in the Computer Information Area. *Pravo. Zhurnal Vysshey shkoly ekonomiki*, no 4, pp. 86–95 (in Russian)

DOI: 10.17323/2072-8166.2016.4.86.95


## References


Dobrovol'skiy V.I. (2014*) Moshennichestvo v sfere kreditovaniya i smezhnye sostavy prestupleniy: voprosy primeneniya i razgranicheniy st. 159.1, 159.3 UK I inykh sostavov prestupleniy* [Fraud in Crediting and Correlated Components of Crime]. SPS Konsul'tantPlyus.

Esakov G.A. (2014) Ugolovnyy zakon i predprinimateli: dostizheniya I proschety [Criminal Law and Entrepreneurs: Achievements and Issues]. *Ugolovnoe pravo i sovremennost'*, vyp. 5, pp.104–122.

Kochoi S.M. (2014) *Prestupleniya protiv sobstvennosti* [Crimes against Property. Moscow: Prospekt, 88 p. (in Russian)

Lopashenko N.A. (2012) *Posyagatel'stva na sobstvennost'* [Infringement of Property]. Moscow: Norma, 527 p. (in Russian)

Lopashenko N.A. (2015) Zakonodatel'naya reforma moshennichestva: vynuzhdennye voprosy i vynuzhdennye otvety [Reform in the Legislation on Fraud: Involuntary Questions and Involuntary Answers]. *Kriminologicheskiy zhurnal Baykal'skogo gosudarstvennogo universiteta ekonomiki i prava*, vol. 9, no 3, pp. 504–513.

Potapkin S.N. et al. (2015) Voprosy ob"ektivnoy storony moshennichestva v sfere komp'yuternoy informatsii v sudebno-sledstvennoypraktike. *Biblioteka nauchnykh publikatsiy elektronnogo periodicheskogo spravochnika*, no 1, SPS Garant.

Shumikhin V.G. (2014) Sed'maya forma khishcheniya chuzhogo imushchestva [Form 7 of Embezzlement of Property]. *Vestnik Permskogo universiteta. Yuridicheskie nauki*, vyp. 2, pp. 229–233.

Smolin S. (2014) Ugolovno-pravovaya bor'ba s vysokotekhnologichnymi sposobami i sredstvami sovershenia prestupleniy. *Ugolovnoe pravo*, no 4, pp. 62–68.

Tret'yak M. (2014) *Moshennichestvo kak prestuplenie protiv sobstvennosti v sovremennom ugolovnom prave: kurs lektsiy* [Fraud as a Crime against Property in Modern Criminal Law: Lectures]. Moscow: Yurlitinform, 200 p. (in Russian)

Tret'yak M. (2015) Problemy kvalifikatsii novykh sposobov moshennichestva [Issues in Classifying New Frauds]. *Ugolovnoe pravo*, no 2, pp. 94–98.

Tret'yak M. (2014) Pravila kvalifikatsii komp'yuternogo moshennichestva I prestupleniy, predusmotrennykh gl. 28 UK RF [Classifying Cyber Frauds and Crimes under Chapter 28 of the RF Criminal Code]. *Ugolovnoe pravo*, no 4, pp. 69–74.

Tyunin V. (2013) «Restrukturizatsiya» ugolovnogo zakonodatel'stva ob otvetstvennosti za moshennichestvo [Restructuring Criminal Law on Liability in Fraud]. *Ugolovnoe pravo*, no 2, pp. 35–41.

Yani P.S. (2015) Spetsial'nye vidy moshennichestva. [Special Types of Fraud]. *Zakonnost'*, no 8, pp. 35–40.

Yuzhin A.A. (2016) *Moshennichestvo i ego vidy v rossiyskom ugolovnom prave. (dis… kand. yurid. nauk.)* [Fraud and its Types in Russian Criminal Law. (Candidate of Juridical Sciences Dissertation)]. Moscow: MGYuA. 238 p.

Zhalinskiy A.E. (2015) Ugolovno-ekonomicheskoe pravo: problematika opredelennosti zakona (rossiyskie I nemetskie vzglyady). *Izbrannye trudy.* T.2. [Criminal and Economic Law: Issues in Law (Russian and German Views) Selected Works]. Vol. 2. Moscow: HSE Publishers, pp. 317–329 (in Russian)