**Проблемы квалификации и расследования мошенничества в сфере компьютерной информации**

**Диплом**

2012

В настоящее время высокие технологии являются неотъемлемой частью практически всех сфер жизнедеятельности человека. Стремительное развитие компьютерных технологий и всеобщая глобальная информатизация общества, с одной стороны, безусловно, имеют положительное значение для общества, но, с другой стороны, порождают ряд негативных последствий, одним из которых выступает криминализация компьютерных и информационно-телекоммуникационных сетей связи.

Оглавление

Введение

Глава 1. Характеристика состава и проблемы квалификации преступления, предусмотренного статьей 159.6 УК РФ

.1 Объект и объективная сторона ст. 159.6 УК РФ. Субъективные признаки ст. 159.6 УК РФ

.2 Квалифицированные составы мошенничества в сфере компьютерной информации

Глава 2. Отграничение состава преступления, предусмотренного статьей 159.6 УК РФ от смежных составов

.1 Отличие статьи 159 УК РФ от статьи 159.6 УК РФ

.2 Отличие ст. 159.6 УК РФ от статей 272 -274 УК РФ

Глава 3. Правовые и криминалистические проблемы расследования мошенничества в сфере компьютерной информации

.1 Особенности производства первоначальных следственных действий и оперативно-розыскных мероприятий при расследовании преступления, предусмотренного ст. 159.6 УК РФ

.2 Обстоятельства, подлежащие установлению при расследовании мошенничества в сфере компьютерной информации

Заключение

Список литературы

Введение

В настоящее время высокие технологии являются неотъемлемой частью практически всех сфер жизнедеятельности человека. Стремительное развитие компьютерных технологий и всеобщая глобальная информатизация общества, с одной стороны, безусловно, имеют положительное значение для общества, но, с другой стороны, порождают ряд негативных последствий, одним из которых выступает криминализация компьютерных и информационно-телекоммуникационных сетей связи. Внедрение современных информационных технологий в различные сферы человеческой деятельности приводит к тому, что при помощи информационно-телекоммуникационных сетей связи совершаются не только преступления в сфере компьютерной информации, предусмотренные главой 28 Уголовного кодекса РФ (далее по тексту — УК РФ), но и «традиционные» преступления — кража, присвоение, мошенничество и другие. Использование компьютерных технологий выступает здесь с отрицательной преступной целью: хищение денежных средств путем перечисления их на фиктивные счета; совершение различных действий с применением фальсифицированных либо похищенных электронных средств платежа; распространение вредоносных программ; мошеннические действия, совершаемые с использованием информационно-телекоммуникационных сетей, включая Интернет и другие действия.

Совершение мошенничества с использованием компьютерной техники набирает обороты ввиду того, что использование компьютерных программ в корыстных целях позволяет обернуть криминальную деятельность к сверхдоходности при наименее безопасной обстановке для преступника. Существующие в настоящее время правила использования киберпространства позволяют злоумышленникам обеспечить себе свободный доступ к многочисленным материальным ресурсам при наличии наиболее скрытой формы преступных действий. Так стремительное развитие информационно-телекоммуникационной сферы не только открыло новые возможности развития человечества, но и вместе с тем породило ряд качественно новых угроз, включая угрозы глобального значения.

В числе первых нормативно-правовых актов, касающихся сферы мошенничества с применением компьютерных технологий, является Конвенция о киберпреступности. Предполагалось, что данный нормативно-правовой акт послужит эталоном для национальных законодателей, выйдя на глобальный уровень ввиду того, что данный документ является первым международным документом, относящимся к данной сфере. Тем не менее, указанный нормативно-правовой акт, объединивший в себе усилия противодействия и борьбы с киберпреступностью, не явился, как предполагалось, универсальным решением существующих и множащихся проблем в данной сфере, а лишь привел к разобщению подходов в гармонизации законодательства. В настоящее время Российская Федерация не ратифицировала данную конвенцию [Распоряжение Президента РФ от 22.03.2008 № 144-рп].

|  |
| --- |
| [Вернуться в библиотеку по экономике и праву: учебники, дипломы, диссертации](http://учебники.информ2000.рф/index.shtml)  [Рерайт текстов и уникализация 90 %](http://учебники.информ2000.рф/rerait-diplom.shtml)  [Написание по заказу контрольных, дипломов, диссертаций. . .](http://учебники.информ2000.рф/napisat-diplom.shtml) |

Безусловно, мошенничество является одним из наиболее распространенных преступных посягательств на собственность в различных сферах экономической деятельности. Закрепление в УК РФ ряда статей, устанавливающих уголовную ответственность за совершение преступлений в сфере компьютерной информации — необходимое действие, продиктованное стремительным развитием компьютерных и информационно-телекоммуникационных технологий, которые в свою очередь порождают новые способы хищений чужого имущества или приобретения права на чужое имущество. Об этом, в частности относительно введения новой статьи 159.6 УК РФ, предусматривающей уголовную ответственность за совершение мошенничества в сфере компьютерной информации, говорится в содержании пояснительной записки к проекту федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации». Из содержания пояснительной записки следует, что совершение мошенничества в сфере компьютерной информации требует определенных уголовно-правовых мер воздействия со стороны государства. Ранее закрепленный в Уголовном кодексе Российской Федерации состав мошенничества («классическое мошенничество», предусмотренное статьей 159 УК РФ) в полной мере не отображал особенности различных экономических отношений, и не мог обеспечить на высоком уровне защиту потерпевших от мошеннических действий.

Эффективное противостояние преступлениям в сфере компьютерной информации возможно при существовании соответствующего правового механизма. Для того чтобы установить тот или иной состав преступления необходимо присутствие в уголовном законодательстве предусмотренной ответственности за такое деяние. В российском уголовном законодательстве уголовная ответственность за преступления в сфере компьютерной информации установлена, прежде всего, в главе 28 УК РФ «Преступления в сфере компьютерной информации». Федеральным законом от 29.11.2012 «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» глава 21 УК РФ, устанавливающая ответственность за преступления против собственности, была дополнена шестью новыми составами мошенничества. В числе таких составов — статья 159.6 УК РФ, предусматривающая уголовную ответственность за совершение мошенничества в сфере компьютерной информации, введенная, прежде всего, в связи с необходимостью установить уголовную ответственность в случаях, когда хищение или приобретение права на чужое имущество непосредственно сопряжено с вмешательством в компьютерные системы.

Безусловно, не вызывает сомнений тот факт, что преступления, которые совершены с помощью компьютерных технологий, имеют свою особую специфику. Применение компьютерных технологий лицами, совершающими подобные преступления, подчеркивает высокую степень общественной опасности данной категории преступлений, как в сфере экономической деятельности, так и в сфере общественных интересов. Распространение преступлений в сфере высоких технологий ставит сотрудников правоохранительных органов перед необходимостью детального изучения сферы компьютерных технологий и их последующего использования в борьбе с преступлениями данной категории дел.

Изменения, внесенные в уголовное законодательство, бесспорно, имеют целью усиление борьбы с новыми видами проявления мошенничества. Введение статьи 159.6 УК РФ обусловлено необходимостью обеспечить защиту интересов собственности (имущественные интересы) лиц, охрану компьютерной информации, а также безопасность информационно-телекоммуникационных сетей. Тем не менее, в настоящее время остается ряд спорных моментов и нерешенных вопросов, касающихся произведенных нововведений. Это порождает ряд проблем при квалификации преступления, предусмотренного статьей 159.6 УК РФ, осложняющих расследование хищений чужого имущества или приобретения права на чужое имущество с использованием компьютерной информации.

**Цель исследования** — выявление существующих проблем квалификации и расследования мошенничества в сфере компьютерной информации, а также всестороннее исследование теоретических и практических вопросов, связанных с применением действующего законодательства в области применения статьи 159.6 УК РФ.

Исходя из цели исследования и для всестороннего ее достижения, были поставлены следующие **задачи**:

проанализировать состав преступления, предусмотренного статьей 159.6 УК РФ;

провести сравнительный анализ составов статей 159 УК РФ и 159.6 УК РФ с целью определения причин, послуживших основанием для дополнения главы 21 УК РФ самостоятельным составом, предусматривающим наступление уголовной ответственности за совершение мошенничества в сфере компьютерной информации, а также установить, имеется ли в действительности конкуренция общей и специальной нормы;

проанализировать и дать общую характеристику составам преступлений в сфере компьютерной информации, предусмотренным главой 28 УК РФ и выявить критерии отграничения данной категории дел от мошенничества в сфере компьютерной информации;

выявить имеющиеся проблемные вопросы законодательной регламентации мошенничества в сфере компьютерной информации;

показать проблематику в области правоприменения статьи 159.6 УК РФ;

рассмотреть основы методики и особенности тактики следственных действий при расследовании мошенничества в сфере компьютерной информации;

выявить особенности проведения следственных действий и оперативно-розыскных мероприятий, вызывающих затруднения для субъектов расследования мошенничества в сфере компьютерной информации;

изучить способы взаимодействия следователей с лицами, обладающими специальными познаниями, при расследовании мошенничества в сфере компьютерной информации;

**Объектом исследования** выступают общественные отношения, складывающиеся в процессе квалификации мошенничества в сфере компьютерной информации, а также криминалистическая характеристика данной категории дел.

**Предметом исследования** выступают актуальные вопросы уголовно-правовой характеристики мошенничества в сфере компьютерной информации, правовые и криминалистические проблемы расследования мошенничества в сфере компьютерной информации, а также использование специальных познаний в сфере компьютерных технологий данной категории дел.

**Степень разработанности темы.**Несмотря на имеющиеся в настоящее время научные разработки, касающиеся квалификации и расследования мошенничества в сфере компьютерной информации, за гранью широкого и глубоко научного анализа остаются еще многие вопросы данной сферы. Исследование проблематики квалификации и расследования данной категории дел носят значимый теоретический и практический характер для практики борьбы с мошенничеством с использованием компьютерных технологий.

Разрешение существующих проблем требуют всестороннего и компетентного обсуждения с привлечением широкого круга лиц. В данном случае нельзя обойтись без привлечения специалистов в области права, высоких технологий, чтобы как можно более точно переложить общие принципы и подходы борьбы с мошенничеством в сфере компьютерной информации на язык уголовного закона, при этом сохраняя его целостность, системность и фундаментальные положения. Если в полном объеме не продумывать законодательные шаги, то в таком случае они будут способствовать, как в настоящее время способствуют, появлению в уголовном законодательстве еще целого ряда так называемых «мертвых» норм, которые способны не исправить существующую ситуацию, но и усугубить ее. Всё это нашло своё отражение в работах Базарбаева Э.М. «Перспективы развития криминалистики с использованием современных информационных технологий при раскрытии и расследовании преступлений» (2015), Демина К.Е., Васильева А.А. «Криминалистические аспекты получения доказательственной информации с электронных носителей данных» (2011), Дворецкого М.Ю. «Уголовная ответственность за мошенничество в сфере компьютерной информации: проблемы теории и правоприменительной практики» (2013), Згадзай О.Э., Казанцева С.Я., Мазурова И.Е. «Актуальные вопросы борьбы с киберпреступностью» (2013), Комарова И.М. «Правовые и криминалистические проблемы расследования мошенничества в сфере компьютерной информации» (2015), Матвейчук Н.С., Бадикова Д.А. «Некоторые аспекты проведения следственных действий при расследовании мошенничеств в сфере компьютерной информации» (2015), Смирновой И.Г., Сачкова Д.И. «Сложности доказывания по делам о преступлениях в сфере компьютерной информации» (2015), Чекунова И.Г. «Компьютерная преступность: законодательная и правоприменительная проблемы компьютерного мошенничества» (2015), Шумихина В.Г. «Седьмая форма хищения чужого имущества» (2014), Южина А.А. «Дискуссионные вопросы мошенничества в сфере компьютерной информации» (2014) и др.

Следует отметить, что в настоящее время существует объективная необходимость разработки рекомендаций, носящих комплексный характер, позволяющих повысить эффективность работы участников предварительного расследования при выявлении и расследовании мошенничества в сфере компьютерной информации. Высокая практическая значимость и недостаточная научная разработанность вопросов темы диссертационного исследования также определяют и обуславливают актуальность исследования.

**Научная новизна** исследования определена тем, что в работе изучены существующие пробелы действующего законодательства, рассмотрены вытекающие из них проблемы в правоприменении, а также предложены пути их разрешения.

**Структура работы** обусловлена целью и задачами исследования и состоит из введения, трех глав, включающих семь параграфов, заключения и списка использованной литературы.

Глава 1. Характеристика состава и проблемы квалификации преступления, предусмотренного статьей 159.6 УК РФ

.1 Объект и объективная сторона ст. 159.6 УК РФ. Субъективные признаки ст. 159.6 УК РФ

Согласно ст. 159.6 УК РФ под мошенничеством в сфере компьютерной информации понимается «хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей» [Уголовный кодекс Российской Федерации, ст. 159.6].

Как верно отмечает Кауфман Ю.С. «включение мошенничества в сфере компьютерной информации в состав главы 21 УК РФ предусматривает в качестве видового объекта отношения собственности, непосредственным объектом выступает чужое имущество или права на него» [Кауфман, 2014, с. 131]. Также следует отметить, что информация с 1 января 2008 года исключена из перечня объектов гражданских правоотношений. Информация, с присущими ей определенными свойствами, не имеет собственника, что находит свое подтверждение и в законах информационной отрасли права. При применении понятия информационного объекта необходимо учитывать, что информация, имея стоимость, не представляет собой имущество (совокупность вещей). Таким образом, в настоящее время не может быть однозначно решен вопрос возможности рассмотрения информационного объекта в качестве предмета мошенничества, что требует дальнейшего изучения и разработки.

Для квалификации преступлений важное значение имеет специфика признаков объективной стороны состава мошенничества, а именно — способ его совершения.

При проведении анализа объективной стороны мошенничества в сфере компьютерной информации было выявлено, что в диспозиции статьи 159.6 УК РФ нет указания на такой способ совершения преступления, как обман и злоупотребление доверием (такой способ совершения преступления предусмотрен ст. 159 УК РФ). Способами совершения преступления, предусмотренными ст. 159.6 УК РФ являются — ввод, блокирование, модификация и удаление компьютерной информации, либо иное вмешательство. Фактически можно говорить о том, что здесь употребляется терминология составов преступлений, предусмотренных статьями 272-274 УК РФ. Верно отмечает Шебанов Д.В. «как видим, ни о каком обмане либо злоупотреблении доверием в диспозиции рассматриваемой статьи речи не идет. И это логично — ведь обмануть машину, то есть бездушную вещь, лишенную психики, невозможно. Чем, прежде всего, отличалось традиционное мошенничество — прямым или виртуальным, но обязательно контактом с живым лицом. В предложенной законодателем норме это становится неактуальным» [Шебанов и др., 2014, с. 199].

Рассмотрим, что понимается под указанными понятиями. Следует отметить, что, к сожалению, в законодательстве в большинстве своем не раскрывается либо раскрывается недостаточно точно их содержание.

Многие авторы предлагают свои варианты, помогающие раскрыть суть данных понятий. Так, под вводом компьютерной информации предлагается понимать размещение сведений в устройствах ЭВМ для их последующей обработки и (или) хранения. Под удалением компьютерной информации понимается «совершение действий, в результате которых становится невозможным восстановить содержание компьютерной информации и (или) в результате которых уничтожаются носители компьютерной информации» [Гладких, 2014, с. 29].

Рассмотрим подробнее, существует ли объективная необходимость отграничения способа хищения чужого имущества или приобретения права на чужое имущество путем ввода компьютерной информации от иных способов совершения мошенничества в сфере компьютерной информации (выделение как самостоятельного способа) либо стоит рассматривать его как составную часть других способов.

На законодательном уровне в настоящий момент отсутствует разъяснение таких понятий как ввод и иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

При проведении анализа и обобщения материалов судебной практики относительно данного вопроса было установлено, что в ряде случаев для описания судами такого способа совершения мошенничества в сфере компьютерной информации как «ввод» используется формулировка «сформировал сообщение специального формата, представленное в форме электрических сигналов для перевода денежных средств» [Приговор по делу №1-157/2015 Серовского районного суда; приговор по делу № 1-31/2015 Талицкого районного суда]. Следует отметить, что ввод тех или иных данных (в целях блокирования, удаления и т.д.) лицом, совершающим преступное деяние, используется практически для любого из способов, предусмотренных ст. 159.6 УК РФ. В связи с этим возникает вопрос: требуется ли в данном случае указание на использование нескольких способов совершения преступления?

В большинстве случаев в судебной практике не применяется совокупность способов, ввод информации отграничивается как самостоятельный способ совершения мошенничества и ввод, представляющий составную часть иных способов (например, модификации, блокирования и т.д.). Рассмотрим данное положение на примере характерного уголовного дела.

М., находясь в офисе продаж Воронежского филиала ОАО «ВымпелКом», путем обмана получил доступ к рабочему компьютеру ОАО «ВымпелКом», на котором была предустановлена программа «Customer Care Back Office» («CCBO»). Данные, относящиеся к программе «CCBO» стали известны ему после ввода заведомо известных ему персональных учетных данных (логина и пароля) действующего сотрудника ОАО «ВымпелКом» — А. М. произвел действия по внесению 12 корректировок (изменений) в программу, в результате чего перечислил 7080 руб. на баланс находящейся в его распоряжении СИМ-карты. Так М. был осужден за то, что, при наличии прямого умысла, направленного на хищение чужого имущества, путем модификации компьютерной информации, при осознании им общественной опасности совершаемых действий, предвидя высокую вероятность и неизбежность наступления общественно опасных последствий и желая их наступления, с целью незаконного завладения денежными средствами совершил указанные преступные действия [Приговор Кировского районного суда по делу № 1-296/2015]. В представленном примере ввод информации полностью охватывается понятием модификации (осужденный вводил информацию для внесения изменений в программу) и самостоятельного значения не имеет. Но, как отмечалось ранее, в ряде случаев судебная практика идет по пути применения совокупности способов совершения рассматриваемого преступления: «Г. осужден за совершение мошенничества в сфере компьютерной информации, то есть хищение чужого имущества путем ввода компьютерной информации и иного вмешательства в функционирование средств хранения, обработки и передачи компьютерной информации, совершенное с использованием своего служебного положения (44 преступления); за совершение мошенничества в сфере компьютерной информации, то есть хищение чужого имущества путем ввода компьютерной информации и иного вмешательства в функционирование средств хранения, обработки и передачи компьютерной информации, совершенное с использованием своего служебного положения, в крупном размере (3 преступления); за совершение мошенничества в сфере компьютерной информации, то есть хищение чужого имущества путем ввода, модификации компьютерной информации и иного вмешательства в функционирование средств хранения, обработки и передачи компьютерной информации, совершенное с использованием своего служебного положения (26 преступлений) <…>» [Постановление Московского городского суда от 28.01.2015 № 4у/7-195/15].

Таким образом, исходя из изложенного, считаем, что ввод информации следует разграничивать: как самостоятельный способ совершения мошенничества в сфере компьютерной информации и как составную часть других способов совершения данного преступления. В таком случае в качестве отграничительного признака будут выступать наступившие в результате ввода информации последствия. В случае если для совершения рассматриваемого преступления вводится информация, которая приводит к полному либо частичному прекращению ее существования, то содеянное следует считать удалением информации. В случае если ввод информации послужил для пользователя временной приостановкой доступа к ней — имеет место блокирование компьютерной информации. В этих двух случаях вменение виновному лицу признака ввода информации представляется излишним. Однако, в случае, если для изъятия имущества было применено введение информации, которое впоследствии не повлекло рассмотренных выше последствий, то содеянное должно квалифицироваться по признаку «ввод информации». Из судебной практики приведем пример использования ввода компьютерной информации как самостоятельного способа совершения рассматриваемого преступления: «М. признан виновным в совершении мошенничества в сфере компьютерной информации, то есть в хищении чужого имущества путем ввода компьютерной информации, с причинением значительного ущерба гражданину» [Апелляционное постановление Московского городского суда от 15.02.2016 по делу № 10-2087/2016].

Блокирование информации «предполагает совершение действий, которые приводят к ограничению или закрытию доступа к компьютерной системе и предоставляемым ею информационным ресурсам, вызывают искусственно созданное затруднение доступа законных пользователей к компьютерной информации, которые не связаны с ее уничтожением. Блокирование и уничтожение компьютерной информации отличается от вывода из строя компьютерной программы. При выводе из строя компьютерной программы программа для ЭВМ может быть доступна как организованная в виде файла информация, а не как объект взаимодействия с пользователем» [Карамнов, 2010, с. 205.].

Под модификацией компьютерной информации следует понимать внесение изменений в компьютерную информацию (или ее параметры) [Методические рекомендации, п. 1]. Проиллюстрируем применение судами понятия «модификация компьютерной информации» на примере уголовного дела № 44у-142/2014: «обвинение М. в хищении чужого имущества путем модификации компьютерной информации (ч. 1 ст. 159.6 УК РФ по двум эпизодам), хищении чужого имущества путем модификации компьютерной информации, совершенном в особо крупном размере (ч. 4 ст. 159.6 УК РФ), совершении сделки с денежными средствами, приобретенными лицом в результате совершения им преступления, в целях придания правомерного вида владению, пользованию и распоряжению указанными денежными средствами или иным имуществом, в крупном размере (ч. 1 ст. 174.1 УК РФ), с которым последний согласился, обоснованно, подтверждается доказательствами, собранными по уголовному делу» [Постановление Президиума Новосибирского областного суда от 12.09.2014 по делу № 44у-142/2014].

Действующим законодательством «разрешены некоторые виды легальной модификации программ, баз данных (следовательно, информации) лицами, правомерно владеющими этой информацией. К таким модификациям относятся модификации:

) в виде исправления явных ошибок;

) совершенные путем внесения изменений в программу, базу данных для их функционирования, осуществленные на технических средствах пользователя;

) в виде частичного преобразования (декомпиляции) программы для установления способности к взаимодействию с другими программами» [Карамнов, 2010, с. 206.].

По своей сути, вмешательство в функционирование средств хранения, обработки, информационно-телекоммуникационные сети, а также в средства передачи компьютерной информации — это ряд неправомерных действий, направленных на нарушение поставленного процесса обработки, хранения, использования, а также передачи и иного обращения с компьютерной информацией.

Одно из решений данного вопроса было предложено В.В. Хилютой. Хилюта В.В. считает, что в закон целесообразно будет ввести специальную норму, которая предусматривала бы ответственность за хищение, не связанное с мошенничеством, при использовании особого способа совершения преступления — путем модификации результатов, предусмотренных для автоматической обработки данных компьютерных систем [Хилюта, 2013, с. 64.]. Обратим внимание на позицию зарубежных законодателей относительно данного вопроса на примере Соединенного Королевства Великобритании. Закон «О мошенничестве» от 2006 года предусматривает следующее: «введение в заблуждение (или любое другое действие, подразумеваемое под ним) может осуществляться в любой форме в отношении любой системы или устройства, сконструированного для приема, обработки и реагирования на любые взаимодействия (даже без непосредственного человеческого участия)» [Ladenburg G. Blackstone’s Guide to Fraud Act 2006. Oxford press, NY, 2007. P. 21].

Произведенный анализ судебной практики выявил наличие определенных трудностей, возникающих у правоприменительных органов в связи с установлением и отражением в обвинении способа совершения мошенничества в сфере компьютерной информации.

Как было обозначено ранее, в диспозиции статьи 159.6 УК РФ отображены способы совершения мошенничества в сфере компьютерной информации, которые выступают в качестве обязательного признака способа совершения преступления. Так, в одних случаях суды, рассматривая уголовные дела данной категории, ограничиваются цитированием диспозиции ст. 159.6 УК РФ, перечисляя полный перечень предложенных законодателем способов. Например, «было возбуждено уголовное дело в отношении неустановленного лица по признакам преступления, предусмотренного ст. 159.6 ч. 4 УК РФ, в связи с хищением денежных средств с расчетного счета ЗАО «<…>» в размере 29 186 186 рублей, открытого в ОАО АКБ «<…>», посредством ввода, удаления, блокирования и модификации компьютерной информации [Постановление Президиума Верховного Суда РФ от 15.07.2015 № 48П15]. В других случаях — одни и те же обстоятельства совершения преступления квалифицируются судами по разным признакам объективной стороны данного деяния.

В качестве иллюстрации обозначенной проблемы приведем в пример несколько характерных уголовных дел. Нередко хищение совершается путем введения набора цифр на номер «900». В одних уголовных делах этот способ описывается как ввод компьютерной информации [Решение по делу 1-363/2014 Октябрьского районного суда], в других — как ввод и иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей [Приговор Дзержинского районного суда по делу № 1-108/2014]. В третьих случаях суды обходят стороной описание способа совершения преступления. В приговоре указано, что «И. с целью хищения чужого имущества, находясь у себя дома, при применении персонального компьютера, имеющего подключение к сети Интернет, с принадлежащего Р. электронного счета в системе «Единый кошелек» путем перечисления на счет платежной системы «Киви-кошелек» похитил денежные средства в сумме 5000 рублей, после чего перечислил данную сумму на свой банковский счет в ОАО «Экспресс-банк» и обналичил посредством снятия через банкомат» [Решение по делу № 1-260/2014 Златоустовского городского суда]. В обозначенном примере отсутствует описание используемого способа получения доступа к чужому расчетному счету. Эту информацию можно установить, ознакомившись с показаниями потерпевшего Р., в которых отражено, что его электронный счет был взломан, а персональные данные изменены.

Также следует обозначить важное замечание, что речь в случае установления ответственности за хищение, не связанное с мошенничеством, при использовании особого способа совершения преступления, идет о новой форме хищения. Завладение имуществом (и/или приобретение права на имущество) здесь сопряжено с внедрением в информационную среду, посредством которой реализовываются различного рода информационные операции, юридическое значение (последствия) которых состоит в получении участниками имущества в виде наличных денег, безналичных денежных средств, иных имущественных прав [Яни, 2015, с. 39]. Так, например, «переквалифицированы действия неустановленного лица с п. «б» ч. 4 ст. 158 УК РФ на ч. 4 ст. 159.6 УК РФ как мошенничество в сфере компьютерной информации, то есть хищение чужого имущества путем ввода компьютерной информации в функционирование средств хранения, обработки или передачи компьютерной информации, совершенного в особо крупном размере», способ совершения преступления неустановленным лицом — хищение из установленного в указанном ТРЦ банковского терминала ОАО АКБ «Национальный Резервный Банк» денежных средств на сумму 3 758 100 рублей» [Постановление Девятого арбитражного апелляционного суда от 22.07.2015 № 09АП-23934/2015]. Также проиллюстрировать завладение имуществом посредством проведения различного рода информационных операций способен следующий пример рассмотрения Свердловским областным судом уголовного дела № 33-7416/2014: «возбуждено уголовное дело по признакам преступления, предусмотренного, ч. 2 ст. 159.6 УК РФ, хищение денежных средств с банковского счета путем вмешательства в обработку и передачу компьютерной информации» [Апелляционное определение Свердловского областного суда от 30.05.2014 по делу № 33-7416/2014].

В диспозиции статьи 159.6 УК РФ законодателем в качестве способа совершения преступления не указан такой способ, как обман или злоупотребление доверием. Это говорит о том, что «состав совершения мошенничества в сфере компьютерной информации не находится в соотношении с составом «классического» мошенничества, а представляет собой самостоятельную форму хищения с присущим ему специфичным, особым способом, отличным и от иных форм хищения чужого имущества» [Шумихин, 2014, с. 231.] . Таким образом, можно говорить о том, что мошенничество в сфере компьютерной информации имеет свой специфический способ совершения преступления, характерными особенностями которого являются:

«воздействие осуществляется непосредственно на компьютерную информацию, а не на сознание потерпевшего;

отсутствует обман, обязательным признаком которого является введение другого лица в заблуждение путем воздействия на сознание (психику) другого человека;

отсутствует передача имущества или приобретение права на имущество с помощью потерпевшего;

орудием преступления признаются информация, средства хранения, передачи и обработки компьютерной информации, а не ложные сведения, передаваемые человеком» [Третьяк, 2015. с. 96].

Нельзя оставить без внимания вопрос: что порождает установленная законодателем формулировка названия ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации»? Определение мошенничества закреплено в ст. 159 УК РФ, но проведенное исследование позволило прийти к выводу, что мошенничество в сфере компьютерной информации имеет отличный от «классического» мошенничества способ совершения хищения. Дословное восприятие формулировки диспозиции ст. 159.6 УК РФ в совокупности с обозначением данного преступления как «мошенничество…» позволяет увидеть, что подобная формулировка словно отображает два способа совершения преступления. Таким образом, можно говорить о том, что в одной главе закреплены два разных определения преступления мошенничество. Исходя из изложенного, предлагаем оптимизировать терминологию ст. 159.6 УК РФ, озаглавив ее «Хищения в сфере компьютерной информации» или, как было ранее верно предложено Шумихиным В.Г.: «Хищение чужого имущества с использованием компьютерной техники или Компьютерное хищение чужого имущества» [Шумихин, 2014, с. 231.].

Пределы действия статьи 159.6 УК РФ устанавливаются, в том числе, посредством толкования специальных терминов, с помощью которых описана объективная сторона деяния. К ним относятся — компьютерная информация, средства ее хранения, обработки или передачи, информационно-телекоммуникационные сети и их функционирование, ввод, удаление, блокирование, модификация компьютерной информации, иное вмешательство в функционирование указанных средств или сетей. К сожалению, указанные дефиниции в законодательстве в большинстве своем не раскрываются либо содержание их неточно. Так, например, понятие «компьютерная информация» содержится в примечании 1 к ст. 272 УК. Под этим понятием, согласно указанной норме, понимаются «сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи» [Уголовный кодекс Российской Федерации, прим. 1 к ст. 272 УК РФ].

Также следует отметить, что в статье 159.6 УК РФ используется такая формулировка, как «иное вмешательство в функционирование средства хранения…». Конкретизирующего толкования данного понятия нигде не приводится. Это может породить возможность неправильного, узкого или, наоборот, расширенного ее толкования. Данный пробел обращает на себя внимание во многих работах специалистов в области права. Степанов М.В., созвучно с другими авторами, отмечает, что «использование в диспозиции обобщающего термина «иное вмешательство в функционирования средства хранения, обработки или передачи компьютерной информации» позволяет сделать вывод о том, что способы совершения преступления могут быть любыми, самыми различными. Данная формулировка неконкретна, что может породить возможность чрезмерно широкого и неправильного применения термина» [Степанов, 2016, с. 176].

На примере судебной практики рассмотрим, насколько широко и неоднозначно может трактоваться понятие «иное вмешательство в функционирование средства хранения».

Вероятность ограниченного понимания и трактовки термина «иное вмешательство в функционирование средства хранения» рассмотрим на примере приговора Грачевского районного суда Ставропольского края от 13 июня 2013 г. по уголовному делу № 1-82/2013. В соответствии с материалами дела, «Нофенко Л.С. было совершено хищение чужого имущества путем ввода компьютерной информации посредством информационно-телекоммуникационных сетей. Нофенко Л.С., с использованием услуги «Мобильный банк» на мобильный телефон было получено сообщение о доступном лимите денежных средств в \*\*\* сумме на банковском счете, который ей фактически не принадлежал (банковский счет был открыт на имя другого лица). Имея умысел на хищение указанной суммы и реализуя его, Нофенко Л.С. использовала принадлежащий ей мобильный телефон, а также сим-карту с абонентским номером, зарегистрированным на имя Д. Как видно из материалов дела, Д. была ошибочно подключена услуга «Мобильный банк» Сбербанка России, тем не менее, это давало право распоряжаться денежными средствами, находящимися на расчетном счете на имя Ш. путем ввода компьютерной информации в форме электронных сигналов — «смс-сообщений» на номер «900» (с использованием телекоммуникационной сети оператора сотовой связи). НофенкоЛ.С. в несколько приемов перечислила (совершила хищение) денежных средств в \*\*\* сумме, которые находились расчетном счете Ш. и принадлежали ей, на счет используемой для этих целей сим-карты, причинив Ш. имущественный ущерб на общую сумму \*\*\* рублей» [Приговор Грачевского районного суда Ставропольского края от 13 июня 2013 г. по уголовному делу № 1-82/2013].

**[Смотрите также:   Дипломная работа по теме "Специфика продвижения средств массовой информации в интернете"](https://sprosi.xyz/works/diplomnaya-rabota-po-teme-speczifika-prodvizheniya-sredstv-massovoj-informaczii-v-internete/" \t "_blank)**

Рассмотрим также иную точку зрения на данное понятие, которая приводится в приводится Апелляционном определении Московского городского суда от 6 мая 2013 г. № 10-2076.

Д. «был признан виновным в совершении девяти мошенничеств в сфере компьютерной информации, то есть хищении чужого имущества путем иного вмешательства в функционирование средств хранения, обработки передачи компьютерной информации и информативно-телекоммуникационных сетей, группой лиц по предварительному сговору, с причинением значительного ущерба гражданину. А именно в том, что вступил в сговор с лицами, дело в отношении которых выделено в отдельное производство на хищение денежных средств со счетов граждан. Получив информацию о счетах граждан и действуя с учетом договоренности Д. изготавливал поддельные доверенности и получал дубликаты сим-карт и пароли. Далее в период времени с 24.10.2011 по 10.12.2011, Д., используя сим-карты и пароли через электронную систему «\*-Онлайн» путем перечисления на счета и банковские карты различных лиц завладел денежными средствами» [Апелляционное определение Московского городского суда от 6 мая 2013 г. № 10-2076].

Обозначим еще одну проблему, связанную с использованием терминологии, в частности термина «удаление» информации. По сути любую «удаленную» информацию можно восстановить, поэтому «следует предпочесть, скорее, формулировку, установленную статьей 272 УК РФ, где используется более определенный и корректный термин «уничтожение» [Южин, 2014, с. 16].

Необходимо отметить также, что Президиум Верховного Суда РФ дал разъяснение, что новые уголовно-правовые составы (статьи 159.1 — 159.6 УК РФ) необходимо понимать «как специальные разновидности общего состава мошенничества, закрепленного в статье 159 УК РФ» [Обзор судебной практики Верховного Суда РФ…]. Тем самым, Президиум Верховного Суда РФ «предоставил подтверждение позиции, согласно которой «юридическая модель статьи 159 УК РФ является матрицей для производных от нее новых юридических конструкций, что в совокупности с ними образует правовую структуру для борьбы с мошенничеством, совершаемым в различных сферах деятельности» [Александрова, 2014, с. 33].

Тем не менее, как было установлено при рассмотрении вышеизложенного материала, нормы статьи 159 УК РФ и 159.6 УК РФ не конкурируют как общая и специальная, поскольку имеются существенные различия в способе совершения преступления и предмета преступлений.

Рассмотрим субъект и субъективную сторону мошенничества в сфере компьютерной информации.

Субъект преступления, предусмотренный статьей 159.6 УК РФ — общий — дееспособное лицо, достигшее возраста шестнадцати лет. Тем не менее, следует специально отметить, что ч. 3 ст. 159.6 УК РФ, ч. 4 ст. 159.6 УК РФ (деяния, предусмотренные ч. 1, ч.2 или ч. 3 ст. 159.6 УК РФ, совершенные организованной группой либо в особо крупном размере) — для особо квалифицированных составов данного преступления — предусмотрен также и специальный субъект. В качестве специального субъекта выступает лицо, обладающее определенным служебным положением. Так, например, «приговором суда Т.В., К. и К. были признаны виновными в совершении мошенничества в сфере компьютерной информации, <…>, организованной группой, в особо крупном размере, а Т.В. также с использованием своего служебного положения. Т.В., ранее не судимый, осужден по ст. 159.6 ч. 4 УК РФ к 6 годам лишения свободы в исправительной колонии общего режима» [Постановление Московского городского суда от 02.09.2016 № 4у-4286/2016].

Сложности с установлением наличия в совершенных лицом деяниях всех признаков состава преступления, предусмотренного статьей 159.6 УК РФ возникают в отношении субъекта преступления ввиду его анонимности. Большое количество уголовных дел приостанавливается ввиду невозможности установления лица, подлежащего привлечению в качестве обвиняемого. Приведем примеры: «руководитель ООО «Космаковка» в тот же день обратился в правоохранительные органы с заявлением о несанкционированном доступе к расчетному счету истца и денежным средствам в сумме 2237800,00 рублей, по результатам проверки которого было возбуждено уголовное дело № 146420 по признакам преступления, предусмотренного ч. 4 ст. 159.6 Уголовного кодекса Российской Федерации, расследование по которому в настоящее время приостановлено за неустановлением лица, подлежащего привлечению в качестве обвиняемого» [Постановление Девятнадцатого арбитражного апелляционного суда от 27.12.2016 № 19АП-7070/2016]; «27.09.2015 уголовное дело приостановлено в связи с не установлением лица, подлежащего привлечению в качестве обвиняемого» [Постановление Восемнадцатого арбитражного апелляционного суда от 07.12.2016 № 18АП-14973/2016].

Субъективная сторона мошенничества в сфере компьютерной информации «выражается форме прямого умысла. Виновное лицо осознает, что завладение чужим имуществом или правами на него производится путем ввода, удаления, блокирования, модификации компьютерной информации либо иным вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей» [Елин, 2013, с. 74]. Тем не менее, указанные выше обстоятельства не обязательно могут означать наличие признаков состава мошенничества в сфере компьютерной информации. Каждый конкретный случай должен быть объективно устанавливать, что лицо, совершившее определенные в диспозиции статьи 159.6 УК РФ действия, заведомо намеревалось использовать полученную информацию в корыстных целях.

При рассмотрении вопроса касательно существующих в настоящее время проблем в сфере законодательной регламентации мошенничества в сфере компьютерной информации было установлено, что внесенные нововведения стали объектом не только критики, но и насмешек со стороны некоторых авторов. Ю.В. Голик и А.И. Коробеев достаточно резко высказали свою позицию по проведенному реформированию: «Как видим, речь идет о конкретизации объекта и предмета мошенничества путем простого наименования сфер деятельности. Однако не очень понятно, почему выделены именно эти сферы активности мошенников. Почему, например, нет сферы ЖКХ, здравоохранения, образования? Ведь именно они вызывают наибольшее беспокойство у наших граждан и в определенном смысле раздражают власть — деньги вкладываются, а отдачи нет! Специалисты утверждают, что таким образом можно расписать от трехсот до шестисот отраслей. Вот кодекс-то «посолиднеет»!» [Голик, Коробеев, 2013, с. 16 — 17]. Подобного мнения придерживается также Минская В.С., говоря о том, что «законодатель дополнил главу 21 УК РФ шестью новыми специальными по отношению к составу, предусмотренному статьей 159 УК РФ, составами преступлений, предусматривающими, как правило, более мягкую уголовную ответственность за мошенничество, совершенное в разных сферах жизни общества. Такое решение законодателя с точки зрения объектов охраны, конструкции составов преступления, новой терминологии представляется необоснованным» [Минская, 2013, с. 36]. Схожей позиции придерживается Шепелов М.А., считая, что «если следовать логике наших законодателей, то в скором будущем мы сможем увидеть новую статью в тексте УК РФ под названием, например, «Мошенничество в оборонной промышленности» [Шепелов, 2015, с. 155]. Ввиду изложенного справедливым будет отметить, что большинство специалистов обозначает различные существующие проблемы, возникшие и имеющиеся в связи с принятыми нововведениями в главе 21 УК РФ. Так, например, Энгельгардт А.А. отмечает, что «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» [Энгельгардт, 2016, с. 92].

1.2 Квалифицированные составы мошенничества в сфере компьютерной информации

Статья 159.6 УК РФ содержит четыре части. Первая часть статьи 159.6 УК РФ в диспозиции раскрывает понятие мошенничества в сфере компьютерной информации. Вторая, третья и четвертая части указанной статьи содержат: квалифицированный состав — часть 2 ст. 159.6 УК РФ предусматривает ответственность за преступление, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба потерпевшему; особо квалифицированные составы — ч. 3 ст. 159.6 УК РФ устанавливает ответственность за преступления, совершенные виновным лицом с использованием своего служебного положения, а равно в крупном размере, ч. 4 ст. 159.6 УК РФ — устанавливает ответственность за преступления, совершенные организованной группой либо в особо крупном размере.

Таким образом, систематизировав изложенное, выделим следующие признаки квалифицированных составов мошенничества в сфере компьютерной информации:

деяние, «совершенное группой лиц по предварительному сговору (ч.2 ст. 159.6 УК РФ);

с причинением значительного ущерба гражданину (ч.2 ст. 159.6 УК РФ);

совершение преступления лицом с использованием своего служебного положения (ч.3 ст. 159.6 УК РФ);

совершение в крупном размере (ч.3 ст. 159.6 УК РФ);

совершение преступления организованной группой (ч.4 ст. 159.6 УК РФ);

совершение в особо крупном размере (ч.4 ст. 159.6 УК РФ)» [Елин В.М., 2013, с. 76].

В рамках данного исследования рассмотрим подробнее особенности квалифицированных составов мошенничества в сфере компьютерной информации.

Применительно к статье 159 УК РФ крупным размером следует считать стоимость имущества, превышающую двести пятьдесят тысяч рублей, а особо крупным — один миллион рублей. В примечании к статье 159.1 УК установлено, что крупным размером для статьи 159.6 УК РФ признается стоимость похищенного имущества, превышающая один миллион пятьсот тысяч рублей, особо крупным размером шесть миллионов рублей [Колоколов Н.А., 2013, с. 10]. Важным здесь является то, что в обоих случаях крупный и особо крупный размер, установленный для преступлений, предусмотренных статьей 159.6 УК РФ в шесть раз больше, чем тот же размер, предусмотренный для статьи 159 УК РФ.

В качестве еще одной особенности квалицированных составов мошенничества в сфере компьютерной информации рассмотрим размеры санкций, установленных для данных составов в соотношении с «классическим» мошенничеством.

Санкции частей 2 и 3 ст. 159.6 УК РФ предусматривают наказание в виде лишения свободы — наказание может быть назначено на срок до четырех и до пяти лет соответственно, против пяти и шести лет лишения свободы, предусмотренных в санкциях частей 2 и 3 статьи 159.6 УК РФ. Как отмечает Ефремова, в связи с этим можно заключить, что «исходя из анализа санкций данных статей, мошенничество в сфере компьютерной информации является менее общественно опасным ввиду установления менее строгих санкций за его совершение» [Ефремова, 2013, с. 20].

Таким образом, открытым остается вопрос — следует ли из изложенного выше, что законодатель относит преступление в сфере компьютерной информации к менее опасным и менее строго наказуемым деяниям, устанавливая границы размеров похищенного имущества и размер санкций для квалифицированных составов мошенничества в сфере компьютерной информации меньше, чем они установлены для «классического» мошенничества и насколько такое установление является объективным в соответствии со сложившимися жизненными реалиями? Считаем верным выказанное Лопашенко Н.А. по данному вопросу мнение: «скорее, законодатель заботился о мошенниках определенных групп, обеспечивая им более льготные условия привлечения к уголовной ответственности» [Лопашенко, 2015, с. 510], нежели о потерпевшей стороне. Проиллюстрируем вышеизложенное на примере характерного уголовного дела: «Согласно примечанию к ст. 159.1 УК РФ крупным размером в статье 159.6 УК РФ признается стоимость имущества, превышающая 1 500 000 рублей. В ходе судебного разбирательства установлено, что размер ущерба при совершении Г. преступных действий 30 марта 2012 года составил 1 287 536 руб. 21 коп., (преступление № 84), а преступных действий от 6 апреля 2012 года размер ущерба составил 315 159 руб. 65 коп. (преступление № 85). Вместе с тем, в описательно-мотивировочной части приговора, при описании преступлений от 30 марта 2012 года и 6 апреля 2012 года, судом указано на совершение данных преступлений в крупном размере, что не соответствует примечанию к ст. 159.1 УК РФ. Таким образом, судебная коллегия приходит к выводу о необходимости изменения приговора в отношении Г. на основании п. 3 ч. 1 ст. 389.15 и п. 2 ч. 1 ст. 389.18 УПК РФ, и снижения наказания за совершение преступлений от 30 марта 2012 года и 6 апреля 2012 года» [Апелляционное определение Московского городского суда от 01.09.2014 по делу № 10-11485]. Судебная коллегия исключила из описательно-мотивировочной части приговора указание на совершение преступлений в крупном размере и снизила Г. наказание за совершение преступлений, предусмотренных ч. 3 ст. 159.6 УК РФ.

Нельзя не согласиться с позицией Кленовой Т.В. в том, что «решение о введении специальных составов преступлений, если оно мотивируется возросшей опасностью деяний, а санкции предлагаются более мягкие, чем санкция общей нормы, является ошибочным» [Кленова, 2014, с. 27].

Резюмируя изложенное, обозначим наиболее общие выводы по вопросам, рассмотренным в рамках Главы 1 настоящего исследования:

) Способами совершения преступления, предусмотренными ст. 159.6 УК РФ являются — ввод, блокирование, модификация и удаление компьютерной информации, либо иное вмешательство. Фактически это говорит о том, что здесь употребляется терминология составов преступлений, предусмотренных статьями 272-274 УК РФ.

) В диспозиции статьи 159.6 УК РФ законодателем в качестве способа совершения преступления не указан такой способ, как обман или злоупотребление доверием. Это говорит о том, что «состав совершения мошенничества в сфере компьютерной информации не находится в соотношении с составом «классического» мошенничества, а представляет собой самостоятельную форму хищения с присущим ему специфичным, особым способом, отличным и от иных форм хищения чужого имущества».

) Пределы действия статьи 159.6 УК РФ устанавливаются, в том числе, посредством толкования специальных терминов, с помощью которых описана объективная сторона деяния. В законодательстве в большинстве своем не раскрывается либо раскрывается недостаточно точно их содержание. Одним из проблемных моментов является то, что все новые нормы мошенничества, в том числе — мошенничество в сфере компьютерной информации, являются бланкетными. В этих нормах не определяются все признаки этих видов преступлений либо дефиниции отсутствующих признаков сформированы в других нормативных актах. Тем не менее, даже в таком случае в законодательстве не всегда возможно найти, что понимается под тем или иным термином.

) В настоящее время в уголовном законодательстве не существует единого термина для обозначения преступлений с использованием компьютерной техники и/ или компьютерных сетей. При исследовании данного вопроса было выявлено, что ряд федеральных законов закрепил дополнения в части внесения в них официального понятия — «преступления, совершаемые с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет», но, тем не менее, вопрос остается открытым. Таким образом, можно заключить, что предпринятая законодательная инициатива позволяет уголовному законодательству идти дальше и иметь развитие в понимании преступлений с использованием компьютерных технологий.

) Сложности с установлением наличия в совершенных лицом деяниях всех признаков состава преступления, предусмотренного статьей 159.6 УК РФ возникают в отношении субъекта преступления ввиду его анонимности; объективной стороны — ввиду использования лицом для совершения преступления компьютерных технологий; с точки зрения субъективной стороны — ввиду возникающих сложностей при установлении формы вины, цели и мотива совершения преступления. Все это не способствует разрешению проблем, возникающих при борьбе с данной категорией преступлений.

) Проблемным моментом является использование в формулировке диспозиции статьи 159.6 УК РФ такого понятия как «иное вмешательство в функционирование средства хранения». Конкретизирующего толкования данного понятия, как отмечалось ранее, нигде не приводится. Это порождает возможность неправильного, узкого или, наоборот, расширенного ее толкования при правоприменении.

) Одна из проблем, встающая перед правоприменителем, также связана с использованием термина «удаление», который закреплен в диспозиции статьи 159.6 УК РФ и является одним из способов совершения указанного преступления. Более конкретизированный и определенный термин «уничтожение» компьютерной информации используется законодателем в статье 272 УК РФ. Предполагается, что использование подобного термина было бы предпочтительно также и для статьи 159.6 УК РФ.

Глава 2. Отграничение состава преступления, предусмотренного статьей 159.6 УК РФ от смежных составов

2.1 Отличие статьи 159 УК РФ от статьи 159.6 УК РФ

Как верно отмечает Кленова Т.В., «даже конкурирующие составы нередко отличаются друг от друга по законодательной технике выражения» [Кленова, 2014, с. 27].

Многие авторы в проведенных ими анализах новелл, касающихся специальных видов мошенничества, обращают свое внимание на то, что все эти составы (ст. 159.1-159.6 УК РФ) являются частными случаями мошенничества (ст. 159 УК РФ). Авторы находят подтверждение тому, что в таком случае имеется соотношение общей и специальной норм. Тем не менее, существуют достаточно аргументированные и обоснованные позиции других авторов, имеющих отличную, противоположную первым точку зрения по данному вопросу. В контексте рассмотрения вопроса — в чем выражается отличие статьи 159 УК РФ от статьи 159.6 УК РФ, обозначим также — является ли состав ст. 159.6 УК РФ частным случаем мошенничества и имеется ли в данном случае конкуренция общей и специальной нормы. Ответ на поставленный вопрос рассмотрим с позиции критериев выделения общей и специальной норм, определив наличие ситуации конкуренции общей и специальной нормы. С помощью этих критериев определим основания отличия мошенничества и мошенничества в сфере компьютерной информации.

Главный критерий, позволяющий не допустить ошибки при определении общей и специальной нормы — признаки объективной стороны преступления, которое предусмотрено общей нормой — должны полностью включать в себя признаки объективной стороны преступления, содержащегося в специальной норме. В качестве «двух дополнительных критериев выступают: основные признаки субъективной стороны (полное совпадение мотивов и целей в таком случае необязательно; должны совпадать формы вины); должно присутствовать частичное совпадение признаков объекта (непосредственный, основной и дополнительный)» [Шумихин, 2014, с. 230].

Для квалификации преступлений важное значение имеют особые, специфические признаки объективной стороны, а именно — способ совершения преступления. При проведении анализа статей 159 и 159.6 УК РФ были выявлены несовпадения в части признаков объективной стороны этих составов. Объективная сторона «классического» мошенничества, предусмотренного статьей 159 УК РФ, предполагает два способа совершения преступления — обман и злоупотребление доверием. Критерии, позволяющие определить способ совершения преступления как обман или злоупотребление доверием, содержатся в пунктах 2, 3 Постановления Пленума Верховного Суда Российской Федерации от 27 декабря 2007 г. № 51 о судебной практике по делам о мошенничестве, присвоении и растрате (далее — Постановление Пленума ВС РФ от 27 декабря 2007 г. № 51). Согласно п. 2 Постановления Пленума ВС РФ от 27 декабря 2007 г. № 51обман подразумевает под собой либо сознательное искажение фактов (активный обман), либо сознательное умолчание об истине (пассивный обман) с целью ввести лицо в заблуждение. В соответствии с п. 3 Постановления Пленума ВС РФ от 27 декабря 2007 г. № 51 под злоупотреблением доверием понимается использование в корыстных целях виновным особых доверительных отношений, сложившихся между ним и собственником (владельцем) имущества. Нельзя не согласиться с суждением Минской В.С., указывающей, что по своему содержанию злоупотребление доверием можно отнести к разновидности обмана, поскольку для создания видимости правдоподобности обмана используются уже сложившиеся ранее доверительные отношения [Минская, 2013, с. 37].

Диспозиция статьи 159.6 УК РФ не предусматривает такие способы совершения преступления как обман и злоупотребление доверием. Обозначив данное преступление как мошенничество, законодатель определил конкретный способ его совершения — хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей [Уголовный кодекс Российской Федерации, ст. 159.6]. Такой способ совершения преступления не предусматривает личностного контакта субъекта и потерпевшей стороны — в данном случае имеют место исключительно манипуляции, которые осуществляет субъект с помощью технических и программных средств. Например, «преступления совершены при следующих обстоятельствах: Г. с 30 апреля 2008 года работая в должности \*\*\*\* ООО «С», а с 29 января 2010 года в должности \*\*\*\* данного Общества, расположенного по адресу: \*\*\*\*, имея доступ к автоматизированному программному обеспечению «С», в котором производится расчет заработной платы иных выплат сотрудникам ООО «С», в период времени с мая 2009 года по апрель 2012 года, используя доступ к компьютерным программам и свое служебное положение, похитил денежные средства ООО «С», в том числе в крупном и особо крупных размерах» [Апелляционное определение Московского городского суда от 01.09.2014 по делу № 10-11485]. Исходя из формулировки диспозиции, можно установить, что мошенничество в сфере компьютерной информации является самостоятельной формой хищения и имеет специфический способ хищения, отличный от других форм хищения.

Таким образом, объективная сторона составов преступлений статей 159 УК РФ и 159.6 УК РФ по указанным логико-конструктивным признакам не совпадает. В таком случае, вывод будет следующим — нормы не находятся в соотношении общей и специальной. Как можно предположить, обстоятельства несовпадения объективной стороны классической формы мошенничества и мошенничества в сфере компьютерной информации также легли в основу закрепления законодателем рассматриваемого состава в отдельной статье УК РФ.

В целом можно говорить о том, что статья 159.6 УК РФ имеет основное юридическое разграничение с «классическим» мошенничеством в способе совершения хищения имущества. Тем не менее, при проведении анализа санкций статей 159 УК РФ и 159.6 УК РФ также были выявлены некоторые особенности, которые следует отметить.

Санкции статьи 159.6 УК РФ практически идентичны санкциям ст. 159 УК РФ, но имеется небольшое отличие. В ч. 1 ст. 159.6 УК РФ не предусмотрен такой вид наказания как лишение свободы, в то время как ст. 159 УК РФ предусмотрен такой вид наказания сроком до двух лет. В санкциях частей 2 и 3 ст.159 УК РФ присутствует наказание в виде лишения свободы сроком на пять и шесть лет соответственно, против сроков наказания до четырех и до пяти лет лишения свободы, предусмотренного в санкциях частей 2, 3 ст. 159.6 УК РФ. Исходя из приведенного анализа санкций данных статей, можно заключить, что законодатель расценивает мошенничество в сфере компьютерной информации как менее общественно опасное, поскольку устанавливает менее строгие санкции за его совершение. Законодатель смягчил уголовную ответственность за мошенничество в сфере компьютерной информации, не предусмотрев в ч. 1 ст. 159.6 УК РФ наказания в виде лишения свободы. Таким образом, наказание за неквалифицированный состав преступления в специальном виде мошенничества остается более мягким по сравнению с «простым» мошенничеством. Это позволяет говорить о некоторой необоснованности смягчения уголовной ответственности за преступление, предусмотренное ч. 1 ст. 159.6 УК РФ. В ч. 4 ст. 159.6 УК РФ изменено понимание особо квалифицирующего признака — особого крупного размера, в связи с чем, к сожалению, можно говорить о том, что это позволило улучшить положение лиц, совершивших мошенничество в сфере компьютерной информации.

.2 Отличие ст. 159.6 УК РФ от статей 272 -274 УК РФ

Рассмотрим отличие статьи 159.6 УК РФ от статей, предусмотренных главой 28 УК РФ и устанавливающих уголовную ответственность за преступления в сфере компьютерной информации.

Статья 272 УК РФ предусматривает уголовную ответственность за неправомерный доступ к компьютерной информации. Объективная сторона преступления, предусмотренного ч. 2 ст. 272 УК РФ (неправомерное использование компьютерной информации из корыстной заинтересованности), имеет некоторое кажущееся сходство с объективной стороной мошенничества в сфере компьютерной информации, в связи с чем возникают вопросы по поводу отграничения ст. 159.6 УК РФ от ч. 2 ст. 272 УК РФ.

Проведем разграничение ст. 159.6 УК РФ и ст. 272 УК РФ по объективной стороне.

Форма объективной стороны преступления, предусмотренного ст. 159.6 УК РФ ограничена законодателем. Как было установлено ранее, объективная сторона мошенничества в сфере компьютерной информации предусматривает особый способ совершения преступления — ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Исходя из смысла диспозиции статьи 272 УК РФ блокирование, уничтожение, копирование и модификация компьютерной информации являются не способом совершения преступления, а обязательными прямыми последствиями совершенного неправомерного доступа к компьютерной информации. Как верно отмечает Третьяк М., в ст. 159.6 УК РФ помимо блокирования, уничтожения, копирования и модификации компьютерной информации, установленных также для ст. 272 УК РФ, указаны также такие способы совершения преступления как «ввод» компьютерной информации и «иное вмешательство» [Третьяк, 2014, с. 72]. Таким образом, можно говорить о том, что перечень признаков преступления, предусмотренного ст. 159.6 УК РФ значительно шире, нежели тот, что приведен в ст. 272 УК, и касающийся общественно опасных последствий, которые наступают в результате неправомерного доступа к охраняемой законом компьютерной информации (исключением в данном случае можно считать копирование, не являющееся признаком компьютерного мошенничества) [Яни, 2015, с. 37].

Введение мошенничества в сфере компьютерной информации представлялось необходимым в свете возрастающих потребностей современного общества, но, тем не менее, в данном отношении существуют множество дискуссионных вопросов. Одним из таких вопросов является замечание многих авторов относительно ее спорного содержания. Подобные вопросы возникают в связи с тем, что обязательный признак объективной стороны мошенничества в сфере компьютерной информации попадает под санкцию ст. 272 УК РФ «Неправомерный доступ к компьютерной информации». В ч. 1 ст. 159.6 УК РФ не предусмотрен такой вид наказания как лишение свободы, в то время как в ч. 1 ст. 272 УК РФ предусмотрен такой вид наказания сроком до двух лет. Некоторые авторы придерживаются позиции, что, в таком случае содеянное следует квалифицировать по совокупности преступлений [Елин, 2013. С. 7]. Данная ситуация порождает противоречивое толкование и применение уголовного законодательства в части квалификации содеянного по совокупности указанных деяний: ст. 159.6 УК РФ и ст. 272 УК РФ. В связи с этим возникает вопрос: возможна ли квалификация преступных действий как идеальная совокупность преступлений, предусмотренных статьями 159.6 УК РФ и 272 УК РФ? Анализ судебной практики по делам о мошенничестве в сфере компьютерной информации также показал отсутствие единообразного подхода к применению данной нормы. Так, например, И. была признана судом виновной в совершении преступлений, предусмотренных ч. 3 ст. 272, ч. 3 ст. 159.6 УК РФ. И. с целью получения выгоды имущественного характера для себя и корыстных побуждений совершила неправомерный доступ к охраняемой законом компьютерной информации, содержащей персональные данные клиентов ОАО «Л» и их лицевых счетов, являясь специалистом офиса продаж и обслуживания ООО «Л». И. была произведена замена сим-карты при отсутствии соответствующего заявления клиента, в результате чего она получила возможность использования лицевого счета абонента с возможность распоряжения находящихся на нем денежных средств [Приговор Октябрьского районного суда г. Самары по делу № 1-153/2014].

Следует отметить, что до введения в УК РФ ст. 159.6 компьютерной мошенничество, согласно пункту 12 постановления Пленума ВС РФ от 27.12.07 г. № 51 квалифицировалось по совокупности статьей 159 и 272 УК РФ [Постановление Пленума Верховного Суда РФ от 27.12.2007 № 51]. Как видно из материалов приведенного дела, в данном случае имеет место двойное вменение. Ст. 159.6 УК РФ полностью охватывается ввод, удаление, блокировка модификации компьютерной информации, совершенные из корыстной заинтересованности, в связи с чем дополнительной квалификации по ст. 272 УК РФ не требуется. Приведем в пример материалы аналогичного уголовного дела. Л. была признана судом виновной в совершении преступления, предусмотренного ч. 3 ст. 159.6 УК РФ. Л., являясь старшим специалистом отдела по работе с корпоративными клиентами умышленно, из корыстных побуждений совершила хищение денежных средств, использовав для реализации преступной цели автоматизированную систему расчетов «Marti». Л. было осуществлено 116 операций по переводу денежных средств с лицевых счетов ключевых клиентов на подконтрольные ей лицевые счета [Приговор Нижегородского районного суда по делу № 1-251/6/2013]. Констатируя вышеизложенное, считаем, что квалификация преступных действий как идеальная совокупность преступлений, предусмотренных статьями 159.6 и 272 УК РФ невозможна. Также считаем о необходимости обратить внимание на такую имеющуюся проблему в отношении ст.ст. 159.6 и 272 УК РФ, поскольку ввиду наличия близких черт, в практике существуют определенные проблемы, возникающие при квалификации мошенничества в сфере компьютерной информации.

Объективная сторона ст. 272 УК РФ выражается в неправомерном доступе к компьютерной информации. Под доступом, в таком случае, понимается «совершение определенных действий, которые могут выражаться в проникновении в компьютерную систему субъектом путем использования специальных технических или программных средств» [Лебедев, 2013, с. 492]. Такое внедрение позволяет преодолеть установленные системы защиты и незаконно использовать действующие пароли, возможные коды для проникновения в компьютер. Также могут быть совершены и иные действия в целях проникновения в систему или сеть под видом законного пользователя. Неправомерность такого доступа означает внедрение в компьютерную информацию лицом, не обладающим правом на получение и работу с данной информацией либо компьютерной системой. Подразумевается, что в отношении такой компьютерной информации управомоченным лицом приняты специальные меры защиты, ограничивающие круг лиц, имеющих к ней доступ.

С субъективной стороны преступления, предусмотренные статьями 272 УК РФ и 159.6 УК РФ, отличаются по направленности умысла. В случае мошенничества в сфере компьютерной информации умысел направлен на хищение чужого имущества или завладение правом на чужое имущество. В случае неправомерного доступа из корыстной заинтересованности — на получение лицом каких-либо определенных сведений, обладание которыми способствует получению определенной выгоды имущественного характера, не связанной с незаконным безвозмездным обращением имущества в свою пользу или пользу других лиц.

**[Смотрите также:   Дипломная работа по теме "Альтернативная гражданская служба"](https://sprosi.xyz/works/diplomnaya-rabota-po-teme-alternativnaya-grazhdanskaya-sluzhba/" \t "_blank)**

Что касается вопроса санкций, назначаемых за совершение данных преступлений, то можно отметить следующее. Санкция, установленная ч. 1 ст. 159.6 УК РФ является менее строгой по отношению к санкциям, установленным в ч. 1 и 2 ст. 272 УК РФ. Ч. 1 ст. 159.6 УК РФ не предусмотрен способ наказания в виде лишения свободы, ч. 1, 2 ст. 272 УК РФ предусмотрено наказание в виде лишения свободы на срок до 2 лет. Можно предположить, что данное обстоятельство обусловлено особым предметом неправомерного доступа, которым является охраняемая законом информация.

Также следует специально отметить, что в диспозиции статьи 159.6 УК РФ не раскрывается понятие компьютерной информации, равно как и понятие информационно-телекоммуникационная сеть. При квалификации состава, предусмотренного ст. 159.6 УК РФ, необходимо обратиться к Примечанию 1 ст. 272 УК РФ. Примечание 1 к ст. 272 УК РФ раскрывает значение понятия компьютерная информация. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи [Уголовный кодекс Российской Федерации, прим. 1 к ст. 272 УК РФ]. Как отмечает Ефремова М.А., «такая формулировка понятия «компьютерная информация» нуждается в изменении и дальнейшей доработке, поскольку на практике нередко возникают проблемы толкования, касающиеся вопроса, что же следует понимать под средствами хранения, обработки или передачи компьютерной информации. Также понятие «иное вмешательство» нуждается в его раскрытии и уточнении, что позволит избежать возникающего в такой связи расширительного толкования данной формулировки» [Ефремова, 2013, с. 20].

Понятие информационно-телекоммуникационная сеть содержится в п. 4 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ об информации, информационных технологиях и о защите информации. Информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники [Федеральный закон № 149]. Тем не менее, следует отметить, что в данном Федеральном законе не закреплено и не раскрыто содержание терминов, выражающих объективную сторону мошенничества в сфере компьютерной информации: ввод, блокирование, удаление, модификация компьютерной информации [Болсуновская, 2015, с.108]. Доктрина уголовного права отражает различные подходы в понимании содержания указанных признаков, что, тем самым, осложняет их правоприменение.

Статьей 273 главы 28 УК РФ установлена уголовная ответственность за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации [Уголовный кодекс Российской Федерации, ст. 273]. Рассмотрим, в чем выражается отличие объективной стороны преступления, предусмотренного статьей 273 УК РФ, от объективной стороны мошенничества в сфере компьютерной информации.

Объективная сторона преступления, предусмотренного статьей 273 УК РФ, «проявляется в совершении одного из следующих действий:

создание компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации;

использование таких компьютерных программ или такой компьютерной информации;

распространение таких компьютерных программ или такой компьютерной информации» [Чекунов, 2015, с. 31]. Обобщить изложенное, видим, что способом совершения преступления для данного преступления является создание, распространение или использование компьютерных программ или иной компьютерной информации. Уничтожение, блокирование, модификация либо копирование компьютерной информации, выступающие в качестве способа совершения преступления, предусмотренного статьей 159.6 УК РФ, а также нейтрализация средств защиты компьютерной информации, выступают здесь в качестве последствий совершенного виновным лицом преступного деяния, но не в качестве способа совершения преступления.

Статья 274 УК РФ предусматривает уголовную ответственность за «нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» [Уголовный кодекс Российской Федерации, ст. 274 УК РФ].

Объективная сторона данного преступления «выражается в следующих трех условиях, выполненных одновременно:

а) лицо нарушило Правила эксплуатации указанного оборудования;

б) деяние повлекло уничтожение, блокирование или модификацию компьютерной информации;

в) деяние причинило крупный ущерб (свыше 1 млн. рублей)» [Уголовное право России, 2015, с. 620]. Совершение данного преступления подразумевает, что посредством вмешательства виновного лица в функционирование информационных коммуникаций разрушаются информационные ресурсы, следствием чего является нарушение работы технологического оборудования. Как видим из приведенного материала, способ совершения преступления, предусмотренного статьей 274 УК РФ, является в корне отличным от способа, установленного для мошенничества в сфере компьютерной информации.

Также отметим, что в качестве обязательного признака для преступления, предусмотренного статьей 274 УК РФ, выступает существенный вред, возникающий вследствие причинения виновным лицом крупного ущерба владельцу ЭВМ, либо пользователю, или же третьим лицам. Согласно пункту 2 Примечания к статье 272 УК РФ крупным ущербом признается ущерб, составляющий не менее одного миллиона рублей. Таким образом, если причиненный ущерб будет составлять менее одного миллиона рублей, то такое деяние не образует состава данного преступления. Что касается преступления, предусмотренного статьей 159.6 УК РФ (при применении ч. 1 ст. 159.6 УК РФ), то постановка вопроса об уголовной ответственности наступает «в случае, если стоимость похищенного имущества превышает одну тысячу рублей» [Дворецкий, 2013, с. 408]. Для части 2 статьи 159.6 УК РФ постановка вопроса об уголовной ответственности наступает в случае причинения виновным лицом потерпевшему значительного ущерба. Размер значительного ущерба, согласно п. 2 примечания к статье 158 УК РФ составляет не менее двух тысяч пятисот рублей, с учетом имущественного положения потерпевшего. Для иллюстрации данного положения рассмотрим одно характерное дело.

Следует также отметить, что в части 2 статьи 272 и части 2 статьи 273 УК РФ законодателем прямо предусмотрен мотив в виде корыстной заинтересованности, что также является характерной отличительной особенностью данных составов преступлений от мошенничества в сфере компьютерной информации.

Мошенничество в сфере компьютерной информации, как видно из проведенного исследования данного вопроса, имеет достаточно большие сходства с нормами, предусмотренными главой 28 УК РФ «Преступления в сфере компьютерной информации». В связи с этим, нельзя не согласиться с позицией, что «в узком смысле понятие компьютерной преступности охватывает преступления в сфере компьютерной информации, уголовная ответственность за которые предусмотрена в гл. 28 Уголовного кодекса Российской Федерации, а в широком смысле включает в себя понятия киберпреступности, интернет-преступности, преступности в сфере компьютерной информации, преступности в сфере информационных технологий» [Скляров и др., 2016, с. 324]. Тем не менее, законодатель поместил ст. 159.6 УК РФ в другую главу, что подчеркивает важность такого объекта как собственность. Нельзя не согласиться с мнением коллектива авторов, что «рассматривая в данном контексте статью 159.6 УК РФ, можно сделать довольно необычный, но логичный вывод: практически любое хищение (кража, мошенничество, присвоение или растрата), совершенное вышеуказанным способом, подпадает под действие этой уголовно-правовой нормы. Если это не так, и мы придерживаемся традиционного определения мошенничества, то смысла в введении ст.159.6 как отдельной нормы УК РФ абсолютно нет, поскольку и следственная и судебная практика показывает, что мошенничества, совершенные с использованием компьютерных технологий, довольно успешно расследовались и рассматривались в судах и по 159 статье УК РФ. Если же мы все-таки примем новый подход, то невооруженным глазом видна необходимость исключения из названия и диспозиции части первой термина «мошенничество». В противном случае возможна громадная неразбериха в деятельности органов предварительного следствия и суда» [Шебанов и др., 2014, с. 200].

Резюмируя изложенное, обозначим основные выводы, сложившиеся в результате рассмотрения вопросов, поставленных в Главе 2 настоящего исследования:

) Одной из характерных особенностей квалифицированных составов мошенничества в сфере компьютерной информации является признание крупным и особо крупным размером, установленным для преступлений, предусмотренных статьей 159.6 УК РФ размера ущерба в шесть раз больше, чем того, который предусмотрен для статьи 159 УК РФ. УК РФ изменено понимание особо квалифицирующего признака — особого крупного размера, в связи с чем, к сожалению, можно говорить о том, что это позволило улучшить положение лиц, совершивших мошенничество в сфере компьютерной информации.

) Особенностью квалицированных составов мошенничества в сфере компьютерной информации являются менее строгие размеры санкций, установленных для данных составов в соотношении с «классическим» мошенничеством и смежными составами.

) Диспозиция статьи 159.6 УК РФ не предусматривает такие способы совершения преступления как обман и злоупотребление доверием. Исходя из формулировки диспозиции, можно установить, что мошенничество в сфере компьютерной информации является самостоятельной формой хищения и имеет специфический способ хищения, отличный от других форм хищения. Объективная сторона составов преступлений статей 159 и 159.6 УК РФ не совпадает. В таком случае, вывод будет следующим — данные нормы не находятся в соотношении общей и специальной. В целом можно говорить о том, что статья 159.6 УК РФ имеет основное юридическое разграничение с «классическим» мошенничеством в способе совершения хищения имущества.

) Наказание за неквалифицированный состав преступления в специальном виде мошенничества остается более мягким по сравнению с «классическим» мошенничеством. Это позволяет говорить о некоторой необоснованности смягчения уголовной ответственности за преступление, предусмотренное ч. 1 ст. 159.6 УК РФ.

) В ч. 4 ст. 159.6 УК РФ изменено понимание особо квалифицирующего признака — особого крупного размера, в связи с чем, к сожалению, можно говорить о том, что это позволило улучшить положение лиц, совершивших мошенничество в сфере компьютерной информации.

) Основной отличительной особенностью объективной стороны преступления, предусмотренного статьей 272 УК РФ от объективной стороны статьи 159.6 УК РФ, является то, что исходя из смысла диспозиции статьи 272 УК РФ блокирование, уничтожение, копирование и модификация компьютерной информации являются не способом совершения преступления, а обязательными прямыми последствиями совершенного неправомерного доступа к компьютерной информации. С субъективной стороны преступления, предусмотренные статьями 272 УК РФ и 159.6 УК РФ, отличаются по направленности умысла.

) Санкция, установленная ч. 1 ст. 159.6 УК РФ является менее строгой по отношению к санкциям, установленным в ч. 1 и 2 ст. 272 УК РФ. Также следует отметить, что при квалификации состава, предусмотренного ст. 159.6 УК РФ, необходимо обратиться к Примечанию 1 ст. 272 УК РФ в целях раскрытия и правильного толкования термина «компьютерная информация».

) Основным отличием статьи 159.6 УК РФ от статьи 273 УК РФ является способ совершения преступления. Так, способом совершения преступления для преступления, предусмотренного статьей 273 УК РФ, является создание, распространение или использование компьютерных программ или иной компьютерной информации. Уничтожение, блокирование, модификация либо копирование компьютерной информации, выступающие в качестве способа совершения преступления, предусмотренного статьей 159.6 УК РФ, а также нейтрализация средств защиты компьютерной информации, выступают здесь в качестве последствий совершенного виновным лицом преступного деяния, но не в качестве способа совершения преступления.

) В качестве обязательного признака для преступления, предусмотренного статьей 274 УК РФ, в отличие от мошенничества в сфере компьютерной информации, выступает существенный вред, возникающий вследствие причинения виновным лицом крупного ущерба владельцу ЭВМ, либо пользователю, или же третьим лицам.

Глава 3. Правовые и криминалистические проблемы расследования мошенничества в сфере компьютерной информации

3.1 Особенности производства первоначальных следственных действий и оперативно-розыскных мероприятий при расследовании преступления, предусмотренного ст. 159.6 УК РФ

Процесс расследования преступлений обычно делится на три этапа: первоначальный, последующий и заключительный. В качестве основания деления на этапы выступает направленность выполняемых на каждом из этапов следственных действий и сопряженных с ними оперативно-розыскных мероприятий. Функциональность обязанностей первоначальных следственных действий обуславливает их значительную роль в методике расследования преступления, устанавливая ключевую позицию на этапах раскрытия преступления.

Интенсивность поиска, обнаружения, закрепления доказательств о событии преступления, изучение его обстоятельств и лиц, совершивших преступное деяние, розыск и задержание подозреваемых — все это определяет основную направленность первоначального этапа расследования преступления. В связи с этим действиям следователя характерны максимальная оперативность и неотложность. Полученная исходная информация, образующая фактическую основу следственной ситуации, обуславливает производство иных, последующих процессуальных действий.

Расследование мошенничества в сфере компьютерной информации охватывает совершение производства значительного числа предусмотренных уголовно-процессуальным законом процессуальных действий.

Процесс расследования данной категории преступлений, как и любого другого преступления, имеет ситуационный характер и представляет собой деятельность, направленную на решение конкретных задач, обусловленных определенными обстоятельствами. Тактика производства следственных и иных процессуальных действий находится в прямой зависимости от специфики совершения преступления.

Если предполагать идеальный вариант рассмотрения уголовных дел по ст. 159.6 УК РФ, то оно должно быть поручено следователю, обладающему глубокими знаниями в сфере компьютерных технологий. Работа органов предварительного следствия и дознания определена решением сложной задачи по раскрытию преступных действий и фиксации доказательственной информации. Расследование, равно как и предупреждение мошенничества в сфере компьютерной информации, представляет собой комплексную проблему. Решение ее требует особых специфических знаний, находящихся на границе знаний высоких технологий и юриспруденции. Высокий уровень знаний и понимания способов совершения мошенничества в сфере компьютерной информации, профессиональный подход к осуществлению следственных действий по установлению обстоятельств совершения данного преступления и обнаружения лиц их совершивших, несомненно, оказывает значительную роль в эффективном расследовании и ведении борьбы с рассматриваемым преступлением [Виноградова, 2015, с. 109]. Однако, как показывает анализ материалов судебной практики и существующая объективная реальность, характеризующаяся отсутствием специальной подготовки следователей, обладающих знаниями «общеюриста» — следователя», привлекаемых к расследованию данной категории дел — наличие специалистов в правоохранительной системе достаточно невелико. Исключение составляют немногочисленные сотрудники, входящие в состав подразделений Управления «К» МВД РФ. Основными направлениями деятельности Управления «К» Бюро специальных технических мероприятий МВД России являются: активное противодействие преступлениям в сфере компьютерной информации; пресечение противоправных действий в информационно — телекоммуникационных сетях, включая сеть Интернет; борьба с незаконным оборотом радиоэлектронных и специальных технических средств; выявление и пресечение фактов нарушения авторских и смежных прав в сфере информационных технологий; борьба с международными преступлениями в сфере информационных технологий и международное сотрудничество в области борьбы с преступлениями, совершаемыми с использованием информационных технологий [Управление «К» МВД России…, 2017]. Таким образом, существующее положение дел выявляет необходимость научной разработки положений и дальнейшей подготовки на их основе практических рекомендаций по расследованию преступлений в сфере компьютерных технологий в целом и, в частности, мошенничества в сфере компьютерной информации. Аналогичной позиции придерживаются многие авторы, отмечая, что «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» [Антонов и др., 2015, с. 213].

Борьба с мошенничеством в сфере компьютерной информации осложнена тем, что способом совершения преступления является использование удаленного доступа к компьютерной информации. Это позволяет преступнику стереть грань между его местом пребывания и местом преступного посягательства, обойти любые территориальные границы. Как показывает анализ судебной практики «в соответствие с п. 3 ч. 1 ст. 220 УПК РФ в обвинительном заключении следователь указывает существо обвинения, место и время совершения преступления, его способы, мотивы, цели, последствия и другие обстоятельства, имеющие значение для данного уголовного дела» [Апелляционное постановление Московского городского суда от 10.11.2014]. Таким образом, считаем, что для расследования данной категории преступлений необходима разработка особой криминалистической теории, методов и методик, способствующих качественному собиранию, анализу и впоследствии — использованию криминалистически значимой информации.

Среди наиболее часто проводимых следственных действий, иных процессуальных действий, оперативно-розыскных мероприятий по делам о мошенничестве в сфере компьютерной информации можно выделить:

проведение осмотра места происшествия, а также предметов и документов; мошенничество следственный розыскной преступление

допрос лиц, процессуальное положение которых определено. В большинстве случаев это допросы потерпевших и свидетелей, а при установлении лиц, совершивших данное преступление — допросы подозреваемых и обвиняемых. Отметим, что допрос указанных лиц при их выявлении может быть проведен и через существенный промежуток времени;

назначение и производство судебных экспертиз. При этом «в 100% случаев назначалась компьютерно-техническая экспертиза; 60% — дактилоскопическая экспертиза; 55% — технико-криминалистическая экспертиза документов; 25 % — трасологическая экспертиза; 10 % досудебных производств — психологическая экспертиза; 5 % — иные экспертизы» [Смирнова, Коломинов, 2015, с. 27];

обыск и выемка (составляет 90 % уголовных дел);

проверка показаний на месте и следственный эксперимент;

проведение очной ставки;

получение образцов для сравнительного исследования;

получение информации с технических каналов связи;

контроль и прослушивание телефонных и иных переговоров. Следует отметить, что «использование данного следственного действия осложнено тем, что из буквального смысла закона не ясно, кому может быть поручено техническое осуществление контроля и записи переговоров — оперативному подразделению правоохранительного органа или же оператору связи, обслуживающему соответствующие сеансы связи» [Стельмах, 2015, с. 5].

и др.

Как отмечает Малик В.И., «в ходе практики расследования преступлений в сфере компьютерной информации определился круг основных действий и их направленность, а также целевые функции» [Малик, 2016, с. 115]. Алгоритм первоначальных следственных действий и оперативно-розыскных мероприятий при расследовании преступления, предусмотренного ст. 159.6 УК РФ, включает в себя:

. Проведение допроса заявителя или лиц, на которых было указано как на возможных свидетелей.

. Разрешение вопроса о вероятности задержания лица, совершившего преступное деяние с поличным и о проведении необходимых в связи с этим мероприятиях.

. Привлечение специалистов для участия в следственных действиях, включая совершение осмотра места происшествия.

. Осмотр места происшествия.

. Проведение оперативно-розыскных мероприятий с целью определения причин, послуживших мотивом совершения преступного деяния, выявления лиц, виновных в его совершении, выявления следов и иных вещественных доказательств.

. Произведение выемки и последующего осмотра средств электронно-вычислительной техники, предметов, материалов, документов (в том числе находящихся в цифровой форме на компьютерно-технических носителях), определяющих производственную операцию, в ходе которой по имеющимся данным совершены преступные действия.

. Проведение допросов свидетелей.

. Проведение допросов подозреваемых, свидетелей, несущих определенную ответственность за конкретно-определенный участок работы, производственную операцию и защиту информации.

. Проведение обысков по месту проживания, а также на рабочих местах лиц, подозреваемых в совершении преступления.

. Назначение экспертиз: судебной компьютерно-технической, бухгалтерской и иных возможных экспертиз.

Как было обозначено ранее, данный алгоритм представляет собой совокупность первоначальных следственных действий и оперативно-розыскных мероприятий, проработка которых является их неотъемлемой составляющей. Следует отметить, что перечисленные следственные действия не являются исчерпывающими, в связи с тем, что сформулировать универсальный алгоритм расследования для любого случая не представляется возможным. Тем не менее, дальнейшие действия планируются и корректируются с учетом информации, которая была получена в ходе исполнения данного алгоритма.

Остановимся на особенностях некоторых обозначенных выше процессуальных действий. Значимое место среди них занимает одно из наиболее распространенных процессуальных действий — допрос. Тактика производства допроса исследуемой категории уголовных дел прямо связана со спецификой механизма совершения преступления данного вида. Рассмотрим, в чем заключается специфика проведения допроса по уголовным делам о мошенничестве в сфере компьютерной информации. Как отмечает Коломинов В.В. «фактором, положительно влияющим на выбор тактики производства допроса, является наличие определённого объема информации о преступном событии, полученного из различных (процессуальных и не процессуальных) источников, например, материалов доследственной проверки, оперативно-розыскных мероприятий и т. п. Кроме того, содержание преступного деяния таково, что при выяснении обстоятельств его совершения необходимо наличие знаний об особенностях механизма преступления, которые зависят от применяемых для его реализации орудий и средств (компьютерно-технические средства). Именно это обстоятельство, по общему правилу, определяет необходимость присутствия при производстве вербальных следственных действий (в данном случае — допроса) специалиста в сфере компьютерной информации (компьютерных технологий)» [Коломинов, 2015, с. 61]. Тем не менее, предполагаем, что присутствие специалиста при проведении допроса может двояко сказаться на его результатах. Консультирование следователя со специалистом в ходе проведения допроса в присутствии допрашиваемого лица может способствовать в получении им информации о механизме и особенностях преступного события, что в дальнейшем может оказать влияние на допрашиваемое лицо тем или иным образом. Негативным последствием здесь может выступать вероятность построения линии защиты и противодействия с подготовкой к дальнейшей их реализации допрашиваемым лицом (подозреваемым, обвиняемым) за время консультаций следователя со специалистом.

Определенные проблемы в ходе допроса подозреваемого или обвиняемого в совершении мошенничества в сфере компьютерной информации, объясняется тем, что присутствии специалиста в сфере компьютерных технологий позволяет получить допрашиваемому лицу определенный повод для деятельного противодействия. У допрашиваемого (в данном случае — подозреваемого или обвиняемого) возникает уверенность в отсутствии у следователя достаточных знаний о механизме и особенностях совершения мошенничества с применением компьютерных технологий с учетом использованных преступником технических возможностей и применённых компьютерно-технических средств, некое стойкое убеждение в его некомпетентности. Кроме того следует отметить, что присутствие специалиста при производстве допроса третьих лиц (специалиста, защитника) в большинстве случаев негативно сказывается на установлении психологического контакта между следователем и допрашиваемым лицом. Тем не менее, специалисты в области права отмечают, что «участие специалиста положительно влияет на результаты следственного действия, полагая, что следственная практика по уголовным делам, должна идти по пути как обязательных предварительных консультаций со специалистами в ходе подготовке к допросам обвиняемых, так и участия специалистов в таких допросах» [Коломинов, 2015. с. 63].

Следует подчеркнуть, что от усмотрения следователя всегда зависит выбор линии поведения при производстве любого следственного действия, в том числе и допроса. Достижению желаемого результата при условии соблюдения всех принципов уголовно-процессуального законодательства способствует организация процесса проведения производства именно следователем. Таким образом, считаем, что производству такого следственного действия как допрос (вне зависимости от категории допрашиваемого лица) должна предшествовать определенная подготовительная работа. Эта работа должна проводиться относительно установления данных, характеризующих личность допрашиваемого лица, его отношения к расследуемому событию, а также отражать глубокое рассмотрение следователем технической стороны мошенничества в сфере компьютерной информации (выявление особенностей и проведение анализа методов, средств совершения преступления; выявление особенностей их применения и реализации; понимание механизма следообразования).

Процесс расследования мошенничества в сфере компьютерной информации, как отмечалось ранее, носит ситуационный характер, находится под непрерывным влиянием информации и полностью зависит от нее. В таком случае информация выступает в качестве основания для постановки задач на каждом конкретном этапе расследования преступления, тем самым формируя следственную ситуацию. Ученые-криминалисты дают различные определения понятию «следственная ситуация». Как отмечает Матвейчук Н.С., «следственная ситуация характеризуется прежде всего объемом и достоверностью исходной криминалистически значимой информации, поэтому действия следователя или оперативного работника должны быть направлены на обеспечение сохранения обстановки и выяснение подробностей инцидента» [Матвейчук и др., 2015, с. 237]. Также в работах ученых-криминалистов можно встретить такие определения понятия «следственная ситуация» как: положение (состояние) расследования, характеризуемое объемом доказательств и информационного материала; динамическая информационная система, элементами которой являются существенные признаки и свойства обстоятельств, имеющие значение для уголовного дела; совокупность данных о событии преступления и обстоятельствах его расследования [Ковтуненко, 2012, с. 239; Обирин, 2014, с. 271; Князьков, 2013, с 38].

Как отмечает Анапольская А.И., «в науке криминалистике типичные следственные ситуации играют немаловажную роль в формировании методик расследования, позволяют разрабатывать направления по их разрешению, делают деятельность следователя целенаправленной» [Анапольская, 2015, с. 133]. В следственной практике существует определенная повторяемость следственных ситуаций, позволяющая создать фундамент для их обобщений и типизации. В криминалистике типичные следственные ситуации представляют большое значение для формирования методик расследования, способствуют разработке направлений их разрешения, придавая действиям следователя целенаправленность. Обобщив изложенное, отметим, что процесс расследования мошенничества в сфере компьютерной информации представляет собой целенаправленную деятельность по выявлению и закреплению криминалистически значимой информации, которая, в свою очередь, оказывает влияние на формирование следственной ситуации. Элементы, формирующие следственную ситуацию, находятся в тесной взаимосвязи между собой. Каждый из этих элементов в определенной степени содержит информацию о другом, что способствует выдвижению обоснованных версий для целенаправленного проведения расследования преступления.

Первоначальный этап расследования мошенничества в сфере компьютерной информации ознаменован проведением ряда важнейших оперативно-следственных мероприятий, правильность организации и проведения которых находится в прямой зависимости от выявления преступников, производящих приготовление к совершению данного преступления, а также добросовестностью процессуального закрепления в уголовном деле в порядке ст. 89 УПК РФ результатов оперативно-розыскной деятельности, могущих иметь важное доказательственное значение. Как отмечает Комаров И.М., «эта часть расследования «скимминговых» преступлений отчасти позволяет фиксировать следы механизма совершения преступного деяния и процессуально конвертировать их в уголовное дело в качестве доказательств» [Комаров, 2015, с 13]. Тем не менее, на этом уровне взаимодействие следствия с оперативными службами очень слабо или практически отсутствует. Считаем, что это является ошибкой, поскольку в доказывании мошенничества с применением компьютерных средств значительное внимание необходимо уделять материальным следам-последствиям использования компьютерно-технических средств.

Как отмечает Белицкий В.Ю., в проведенных в настоящее время научных исследованиях, касающихся проблематики раскрытия, расследования и судебного разбирательства мошенничества в сфере компьютерной информации как цельного социально-правового явления не подвергались достаточному изучению [Белицкий, 2015, с.4]. Существующие в настоящий момент методики раскрытия и расследования мошенничества с использованием компьютерной информации оказывают незначительное влияние на качество раскрытия и расследования данных преступлений. Следствием этого выступает снижение количества раскрытых уголовных дел данной категории и отсутствие значимого результата по расследованным и направленным на рассмотрение в суд уголовным делам. Таким образом, в настоящее время существует необходимость разработки методик с учетом последних достижений в области криминалистики, изменений уголовного и уголовно-процессуального законодательства, а также обязательным содержанием в них научно обоснованных криминалистических рекомендаций относительно методики раскрытия, расследования и судебного разбирательства таких преступлений.

3.2 Обстоятельства, подлежащие установлению при расследовании мошенничества в сфере компьютерной информации

Реализация предоставляемых действующим российским уголовно-процессуальным законодательством возможностей собирания доказательств в ходе расследовании мошенничества в сфере компьютерной информации, наряду с другими преступлениями в сфере компьютерной информации, имеет ряд существенных трудностей, требующих их разрешения.

В настоящем исследовании рассмотрим обстоятельства, подлежащие установлению и доказыванию при расследовании мошенничества в сфере компьютерной информации, представляющие наиболее высокую сложность при осуществлении расследования.

В ходе проведения расследования преступления должен быть разрешен вопрос о том, что подлежит в данном случае установлению и доказыванию. При проведении анализа судебной, а также следственной практики было установлено, что определенная сложность при расследовании мошенничества в сфере компьютерной информации возникает при установлении места совершения преступления. Следует отметить, что традиционно, место совершения преступления в криминалистике понимается как « участок местности или помещение, где было совершено преступление» [Белкин, 2000, с. 62]. В случае расследования преступления, предусмотренного ст. 159.6 УК РФ, также представляется необходимым рассмотрение понятия «место происшествия», определяемым в традиционной криминалистике как «участок местности или помещение, где были обнаружены следы события, требующего расследования» [Белкин, 2000, с. 62].

Как верно отмечает Коломинов В.В., основная особенность рассматриваемого элемента криминалистического знания выражается в том, что место совершения преступления выступает в качестве носителя материальных и идеальных следов, обладает значимой информативностью и оказывает влияние на весь процесс формирования следовой картины [Коломинов, 2015, с. 265].

Компьютерная сеть обладает рядом специфических особенностей функционирования, что позволяет прийти к следующим выводам:

информационно-телекоммуникационная сеть выступает в качестве места совершения преступления, поскольку именно в ней происходят действия, составляющие объективную сторону мошенничества в сфере компьютерной информации;

местонахождение отдельного компьютера, при помощи которого был совершен неправомерный доступ, также является местом совершения преступных действий, сосредотачивающее в себе следы совершения преступления — основной объем информации, характеризующий процесс совершения преступления (способ совершения преступления, средства и орудия его совершения и т.д.).

Тем не менее, помимо изложенного выше, совершение мошенничества в сфере компьютерной информации часто сопряжено также с наличием еще как минимум одного или нескольких устройств, вовлеченных в процесс обмена информацией с целью выявления необходимых для совершения преступного деяния сведений. При этом фактическое расстояние между местонахождением этих устройств может быть достаточно велико. Данная ситуация очевидным образом негативно сказывается на процессе выявления, расследования и раскрытия мошенничества в сфере компьютерной информации. Исходя из изложенного, считаем, что местом совершения преступления мошенничества в сфере компьютерной информации является местонахождения компьютерно-технических средств, с которых совершается преступное деяние посредством направления определенных команд. Однако, такое определение места совершения рассматриваемого преступления не является окончательным, а его составляющей.

Как верно отмечает Коломинов В.В., высокую значимость для формирования криминалистического знания о преступлении, предусмотренном ст. 159.6 УК РФ, представляет местонахождение компьютерно-технических средств потерпевшего, что обусловлено спецификой преступной деятельности мошенников и характером функционирования системы, в которой происходит ее реализация [Коломинов, 2015, с. 267]. Следует отметить, что ранее в качестве потерпевших от мошенничества с применением компьютерно-технических средств в большей степени выступали юридические лица, в настоящее время все более часто регистрируются инциденты в отношении физических лиц [Лутовинов, 2015, с. 332]. Компьютерно-технические средства лица, на которые оказывалось преступное воздействие, представляют интерес постольку, поскольку компьютерная техника потерпевшего выступает в качестве источника следов и иной информации оказанного преступного воздействия. Это выявляет взаимосвязь места совершения мошенничества в сфере компьютерной информации с техническими средствами, посредством которых оно совершается. Например, в месте нахождения лица, осуществляющего преступные действия в виде неправомерного доступа к компьютерной информации с целью совершения хищения чужого имущества, возможно обнаружить широкий спектр следов подозреваемого — следы пальцев рук на компьютерной технике и иных сопутствующих объектах, запаховые следы и т.д., в месте нахождения потерпевшего-это будут его компьютерно-технические средства. Таким образом, считаем, что многочисленные информативные составляющие места совершения преступления имеют характерное значение для формирования криминалистического знания о мошенничестве в сфере компьютерной информации, а также расследования данного преступления.

**[Смотрите также:   Дипломная работа по теме "Анализ англоязычных текстов музейных буклетов Великобритании и Соединенных Штатов Америки"](https://sprosi.xyz/works/diplomnaya-rabota-po-teme-analiz-angloyazychnyh-tekstov-muzejnyh-bukletov-velikobritanii-i-soedinennyh-shtatov-ameriki-3/" \t "_blank)**

В связи с открытым доступом к сети Интернет значительная часть мошенничеств с применением компьютерных средств совершается именно с использованием сети Интернет, поскольку возможность отследить лицо, совершившее преступление, представляет большие затруднения. Рост данной категории преступлений в России обусловлен отсутствием необходимого взаимодействия правоохранительных органов в вопросах расследования этих преступлений. Аналогичной позиции придерживается и Филимонов С.А. в работе, посвященной проблемам борьбы с компьютерным мошенничеством [Филимонов, 2014, с. 125]. Такое положение еще раз подтверждает необходимость систематического повышения профессиональной подготовки сотрудников правоохранительных органов по вопросам расследования преступления, предусмотренного ст. 159.6 УК РФ.

Определенную сложность при раскрытии и расследовании мошенничества в сфере компьютерной информации в таком случае представляет отслеживание (установление) «IP-адреса» нахождения компьютера, с которого был осуществлен выход в сеть с целью совершения хищения чужого имущества или приобретения права на чужое имущество посредством применения компьютерной техники. Практически каждое уголовное дело, связанное с сетью Интернет, сопряжено с такой оперативно-розыскной задачей, как установление по известному IP-адресу компьютера, использующего его, а также его местоположение. Цепочка доказательств в таком случае выглядит следующим образом: совершенное преступление — IP-адрес — компьютер — человек. IP-адрес в данном случае фиксируется при помощи различных технических средств, с которого было осуществлено преступное деяние. Впоследствии устанавливается компьютер, использовавший данный IP-адрес (факт такого использования закрепляется экспертизой). Следующий шаг — доказывание факта использования (управления) лицом, подозреваемым в совершении преступления этим компьютером.

В ряде случаев IP-адрес является особым способом идентификации компьютера или иного устройства в сети Интернет. Это означает, что только один компьютер может использовать конкретно-определенный IP-адрес в рамках всей глобальной компьютерной сети в каждый (определенный) момент времени.

Как отмечает Федотов Н.Н., «из этого правила имеется целый ряд исключений:

приватные, или так называемые «серые» IP-адреса;

коллективные, или мультикастовые (multicast) IP-адреса;

сетевые и широковещательные (broadcast) IP-адреса;

не выделенные или не присвоенные регистратором IP-адреса;

IP-адреса, относящиеся к территориально распределенным кластерам

компьютеров.

Важнейшими объектами криминалистического исследования в настоящее время, помимо стационарной компьютерной техники и систем, находящихся во взаимосвязи с локальными и глобальными сетями, являются мобильные телефоны сотовой связи, планшетные компьютеры, смартфоны, поскольку ввиду своего повсеместного распространения и наряду с тем, что они являются предметами и орудиями совершения преступлений, они также выступают как носители и средства передачи криминалистически значимой информации.

Определенные свойства цифровых данных обусловливают необходимость следования определенным правилам при фиксации и изъятии цифровых доказательств, а также их судебно-экспертном исследовании. Доказательственная информация, хранящаяся в цифровом виде, обладает определенными отличительными чертами:

неопределенный вид и необходимость использования специальных средств для обеспечения ее восприятия;

вероятность совершить уничтожение или модификацию в минимально возможные сроки, в том числе удаленно;

наличие специальных средств, минимизирующих доступ к данной информации;

непрерывное видоизменение информации в ходе работы пользователя, выполнения всевозможных операций;

формирование взаимосвязанной информации на различных устройствах одновременно при передаче данных по каналам связи.

Как отмечают Россинская Е.Р., Шамаев Г.П. «основные принципы, которыми следует руководствоваться при проведении следственных действий, сопряженных с изъятием компьютерных средств и систем это:

не должна изменяться никакая информация, содержащаяся на изымаемых носителях компьютерной информации;

доступ к информации и исследование ее на месте допустимо только когда невозможно изъять носитель для производства судебной экспертизы;

любые манипуляции с компьютерными средствами и системами должны осуществляться только с участием специалиста;

все выполняемые действия должны подробно протоколироваться, чтобы обеспечить возможность использования результатов этих действий в доказывании» [Россинская, Шамаев, 2014, с. 323].

3.3 Использование специальных познаний при расследовании мошенничества в сфере компьютерной информации

Невысокий уровень борьбы с преступлениями в сфере компьютерных технологий, в частности, рассматриваемого в рамках настоящего исследования мошенничества в сфере компьютерной информации, на наш взгляд, может быть объяснено рядом причин, носящими объективный и субъективный характер. Главной причиной среди объективных выступает природа указанных преступлений — характерное значение здесь имеет особая среда совершения преступления, имеющая специфический механизм и особое следообразование. Это вызвано, прежде всего, особенностями цифровой информации, обрабатываемой с помощью компьютерной техники и передаваемой посредством информационно-телекоммуникационных сетей. Такое положение определяет особую актуальность наличия специальных знаний в процессе выявления и расследования мошенничества в сфере компьютерной информации. Наличие глубоких, специальных знаний необходимо на всех этапах расследования, поскольку криминалистическая характеристика рассматриваемого преступления определена фактором постоянного нарастающего движения в развитии высоких информационных технологий.

В качестве одного из способов использования специальных знаний в уголовном процессе выступает привлечение специалиста к производству определенных следственных действий в целях оказания помощи следователю при обнаружении, изъятии, фиксации следов преступления. Пунктами 5, 6 Федерального закона от 28.07.2012 № 143-ФЗ О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации введено обязательное участие специалиста при производстве обыска и выемки с изъятием электронных носителей информации, а также установлены дополнительные гарантии прав законных владельцев информации [Федеральный закон № 143]. Однако данная мера не решила имеющихся проблем. Следует отметить, что законодатель, сформулировав нормы в ст. 182 Уголовно-процессуального кодекса РФ (далее — УПК РФ) определенным образом обязал следователя привлекать к участию в следственных действиях специалиста во всех случаях изъятия электронных носителей информации. Законодатель не разграничил при этом возможность изъятия электронных носителей информации, подразумевающую под собой безотлагательное участие специалиста — в целях избежания изменения информации, содержащейся на изымаемом носителе (в случае изъятия информации, в которую могут быть внесены какие-либо изменения при совершении следственного действия некомпетентным лицом) и изъятие тех носителей информации, которые могут быть осмотрены и изъяты следователем самостоятельно без нанесения ущерба информации. Нехватка специалистов для участия в каждом следственном действии при их законодательно установленном однозначном и безоговорочном участии ставит под вопрос применение следователем тактических приемов при изъятии носителей цифровой информации, что вынуждает следователя время производства следственного действия определять не исходя из тактических соображений, а из наличия свободного специалиста. В совокупности с имеющейся острой проблемой нехватки экспертов и специалистов, проводящих экспертизы в данной сфере, такое положение вызывает субъективную проблему невысокой эффективности противодействия преступлениям в сфере высоких технологий в целом, а также, в частности, мошенничества в сфере компьютерной информации. Тем не менее, как верно отмечает Кушниренко С.П. «использование специальных знаний выходит на первый план при выявлении и расследовании киберинцидентов и должно учитываться при разработке криминалистических программ организации их выявления и начального этапа расследования, когда уголовно-правовая квалификация совершенного преступления еще не ясна» [Кушниренко, 2015, с. 490].

Расследование и раскрытие мошенничества в сфере компьютерной информации все же не представляется возможным без привлечения специальных познаний в области современных информационных технологий. Существуют мнения, что «следователь или судья, обладая специальными познаниями и соответствующими научно-техническими средствами, в принципе, могут обойтись без помощи специалиста» [Базарбаев, 2015, с. 111]. Тем не менее, не согласимся с приведенной точкой зрения, поскольку при расследовании мошенничества в сфере компьютерной информации наличие специальных познаний следователя может быть недостаточным, что может привести к безвозвратной потере ценной розыскной и доказательственной информации в случае совершения им малейшего неквалифицированного действия. Так, например, Шевченко Е.С. отмечает, что «результаты опроса следователей показали, что у 95% респондентов имеется только юридическое образование, другая дополнительная подготовка ими получена не была, что не может не влиять на качество расследования. Только 5% из числа опрошенных имели еще и образование по специальности «Информатика и вычислительная техника». Из числа опрошенных 63% оценивают свой уровень владения персональным компьютером как уровень «среднего пользователя», 37% считают, что они обладают знаниями «продвинутого пользователя». При этом 79% опрошенных следователей назвали источником знаний компьютерных технологий самообразование, 21% — курсы повышения квалификации сотрудников правоохранительных органов, 5% — коммерческие курсы или специальное образование» [Шевченко, 2015, с. 29].

Несовершенство и недостаточность специальных познаний, как отмечается специалистами в области права, обусловлено учебными программами, «взращивающими» будущих следователей. Как верно указывает Стоянов Р.В., «возбудить дело — это еще далеко не победа. Раскрытие большинства киберпреступлений буксует из-за отсутствия в ряде органов внутренних дел ресурсных возможностей, пока еще недостаточного профессионализма их сотрудников» [Стоянов, 2012, с. 29].Так, Черкасов В.Н. отмечает, что «как бы ни менялись времена, виды и способы совершения преступлений, квалификация преступников и сыщиков, пропасть между расследованием «по линии УР» (назовем это так) и экономическими преступлениями есть сейчас и, наверняка, будет всегда. Любому практику это известно. Теоретику — тоже. Но когда речь заходит об учебных программах, мы продолжаем готовить некоего «общеюриста»-следователя» [Черкасов, 2016. с. 28].

Высокая динамика роста преступлений, совершаемых с применением высоких технологий, опережает процессы раскрытия и расследования данной категории дел. Сложившееся положение «требует от правоохранительных органов, учебных и научных заведений оперативного изучения проблемы, выработки эффективных мер, включающих в себя качественную подготовку необходимых специалистов, отвечающих современному уровню развития информационных сред» [Демин и др., 2011. с. 147].

Обратим внимание на вопрос различия процессуальной и не процессуальной форм деятельности специалистов. Как отмечается, «специалисты в ряде случаев (например, при проверке до возбуждения уголовного дела) также проводят исследования, но они называются предварительными и полученные результаты не имеют доказательственного значения. Такая форма использования специальных познаний не является процессуальной. Не процессуальной по форме является и справочно-консультационная деятельность специалиста [Базарбаев, 2015, с. 111]. В качестве основной процессуальной формы использования специальных познаний выступает судебная экспертиза. К числу основных задач следователя в таком случае относятся: поиск, фиксация и изъятие с помощью специалистов, а в последствии — представление эксперту необходимых материальных объектов — носителей информации.

При подготовке специалистов «для обеспечения раскрытия и расследования преступлений в сфере высоких технологий особое внимание необходимо уделить такой категории как судебные эксперты, которые в данном случае специализируются в новом роде судебных экспертиз со специальные познания целого ряда научных направлений (электроника, электротехника, информационные системы и процессы, радиотехника и связь, автоматизация, вычислительная техника, программирование)» [Базарбаев, 2015, с. 111].

Специалисты (эксперты) с присущими им специальными знаниями в сфере высоких технологий способны внести в деятельность сотрудников правоохранительных органов (в частности — следователей) неоценимый вклад, отражающийся на установлении истины при расследовании преступлений. Существующая объективная реальность отображает неспособность следователей эффективно работать, опираясь исключительно на собственные знания и навыки компьютерных технологий, в большинстве случаев, находящиеся на уровне пользователя. Следователь, даже обладающий знаниями в сфере высоких технологий на уровне уверенного или продвинутого пользователя, едва ли сможет на высоком уровне решить задачи, ставящиеся перед экспертами для проведения экспертизы, например: «из заключения экспертов М. и Я. (№ \*) и показаний эксперта М. в судебном заседании усматривается, что в ходе исследования накопителя на жестких магнитных дисках (НЖМД ООО «\*») установлено, что в базе платежных поручений системы ДБО «\*» обнаружены данные о платежных поручениях, на НЖМД обнаружена программа «\*», которая предоставляет возможность удаленного подключения к ОС по протоколу «\*» с использованием учетной записи «\*». Программа создана в файловой системе 14.11.2011 г. На исследуемом НЖМД обнаружены следы работы этой программы и подключения под учетной записью «\*» в количестве 6 раз 15.11.2011 г. Также обнаружены снимки экрана, созданные 15.11.2011 г., с отображением рабочего стола с системным временем, на которых изображено окно подключения по протоколу «\*» к IP-адресу \* и переписка под учетной записью «\*» с учетной записью «\*» с указанием реквизитов платежного поручения, которые совпадают со сведениями о платежных поручениях, приведенных в постановлении следователя. На одном из них на заднем фоне виден фрагмент страницы веб-браузера «\*», который имеет сходство с панелью администрирования «бот-сетью». В результате анализа содержимого каталогов и файлов на НЖМД, а также сканирования НЖМД с помощью антивирусной программы обнаружено ПО, которое, по мнению эксперта, имеет отношение к инциденту» [Апелляционное определение Московского городского суда от 22.12.2016 по делу № 10-18451/2016].

Обстоятельства рассматриваемых дел могут потребовать глубокого уровня знаний в различных областях компьютерных технологий и возможно возникновение ситуаций, когда будет недостаточно даже знаний привлекаемого специалиста (эксперта). На ряду с тем, что обязанности поиска и закрепления доказательств лежат на следователе, эффективность производства определенных следственных действий (к таким следственным действиям можно отнести обыск, выемку, осмотр места преступления и др.) в ходе расследования мошенничества в сфере компьютерной информации имеет прямую зависимость от процесса организации взаимодействия следователя и специалиста, привлеченного в качестве участника данных мероприятий.

Невозможность создания универсальных рекомендаций с потенциалом их эффективного применения во всех случаях обусловлена постоянным беспрерывным развитием, изменением и обновлением, происходящем в сфере высоких технологий. Такое обстоятельство выявляет необходимость дальнейшей разработки тактических приемов использования помощи лиц, обладающих специальными знаниями в области компьютерных технологий.

В настоящее время в литературе, направленной на рассмотрение вопросов расследования преступлений, совершенных с применением компьютерных технологий, различными авторами сформирована криминалистическая характеристика неправомерного доступа к компьютерной информации, представлены различные классификации неправомерного доступа к компьютерной информации и способов совершения данной категории преступлений, собраны и структурированы данные о способах сокрытия, средствах, орудиях совершения преступлений, разработаны ряд методик, касающихся исследования, обыска компьютерной техники. Тем не менее, одной теоретической и практической значимости данных исследований для расследования и раскрытия мошенничества в сфере компьютерной информации более чем недостаточно. Применение следователем различных методик при исключении из работы специалиста может привести к необратимым потерям вещественных доказательств, значимой информации ввиду недостаточной квалификации следователя в данных вопросах. Большинство авторов, рассматривающих в своих работах вопросы расследования преступлений в сфере компьютерной информации — в общем, и мошенничества в сфере компьютерной информации — в частности, прямо указывают на бесспорную целесообразность привлечения специалистов к расследованию данных преступлений.

Исходя из полученной информации в ходе проведения исследования по данному вопросу, считаем, что специалистов в области компьютерных технологий необходимо привлекать во всех случаях, когда сложившаяся следственная ситуация требует производства действий с использованием специальных знаний указанной категории.

Резюмируя изложенное, обозначим наиболее общие выводы по вопросам, рассмотренным в рамках Главы 3 настоящего исследования:

) Расследование, равно как и предупреждение мошенничества в сфере компьютерной информации, представляет собой комплексную проблему. Решение ее требует особых специфических знаний, находящихся на границе знаний высоких технологий и юриспруденции.

) Борьба с мошенничеством в сфере компьютерной информации осложнена тем, что способом совершения преступления является использование удаленного доступа к компьютерной информации. Это позволяет преступнику стереть грань между его местом пребывания и местом преступного посягательства, обойти любые территориальные границы.

) Присутствие специалиста при проведении допроса может двояко сказаться на его результатах. Консультирование следователя со специалистом в ходе проведения допроса в присутствии допрашиваемого лица может способствовать в получении им информации о механизме и особенностях преступного события, что в дальнейшем может оказать влияние на допрашиваемое лицо тем или иным образом. В исследовании подробно изложены возможные негативные последствия присутствия специалиста при осуществлении такого следственного действия как допрос.

) Взаимодействие следствия с оперативными службами очень слабо или практически отсутствует. Считаем, что это является ошибкой, поскольку в доказывании мошенничества с применением компьютерных средств значительное внимание необходимо уделять материальным следам-последствиям использования компьютерно-технических средств.

) При проведении анализа судебной, а также следственной практики было установлено, что определенная сложность при расследовании мошенничества в сфере компьютерной информации возникает при установлении места совершения преступления. Данный вопрос подробно рассмотрен в исследовании.

) Определенную сложность при раскрытии и расследовании мошенничества в сфере компьютерной информации в таком случае представляет отслеживание (установление) «IP-адреса» нахождения компьютера, с которого был осуществлен выход в сеть с целью совершения хищения чужого имущества или приобретения права на чужое имущество посредством применения компьютерной техники.

) Главной причиной невысокого уровня борьбы с мошенничеством в сфере компьютерной информации выступает природа преступления, предусмотренного ст. 159.6 УК РФ — характерное значение здесь имеет особая среда совершения преступления, имеющая специфический механизм и особое следообразование.

) Способом использования специальных знаний в уголовном процессе является привлечение специалиста к производству определенных следственных действий в целях оказания помощи следователю при обнаружении, изъятии, фиксации следов преступления. Специалисты (эксперты) с присущими им специальными знаниями в сфере высоких технологий способны внести в деятельность сотрудников правоохранительных органов (в частности — следователей) неоценимый вклад, отражающийся на установлении истины при расследовании преступлений. Существующая объективная реальность отображает неспособность следователей эффективно работать, опираясь исключительно на собственные знания и навыки компьютерных технологий, в большинстве случаев, находящиеся на уровне пользователя.

Заключение

В начале исследования перед нами была поставлена цель выявить проблемы квалификации и расследования мошенничества в сфере компьютерной информации, а также всестороннее исследовать теоретические и практические вопросы, связанные с применением действующего законодательства в области применения статьи 159.6 УК РФ.

Подводя итог проделанной работе, и исходя из названной цели и вытекающих из нее задач, можно сформулировать следующие наиболее общие выводы.

Введение статьи 159.6 УК РФ обусловлено прежде всего необходимостью обеспечить защиту интересов собственности (имущественные интересы) лиц, охрану компьютерной информации, а также безопасность информационно-телекоммуникационных сетей. Тем не менее, в настоящее время остается ряд спорных моментов и нерешенных вопросов, касающихся произведенных нововведений. Это порождает ряд проблем при квалификации преступления, предусмотренного статьей 159.6 УК РФ, которые осложняют расследование хищений чужого имущества или приобретения права на чужое имущество с использованием компьютерной информации.

В ходе проведения исследования в рамках первой главы были рассмотрены: общая характеристика состава преступления, предусмотренного статьей 159.6 УК РФ, объективная сторона ст. 159.6 УК РФ, субъективные признаки ст. 159.6 УК РФ, а также квалифицированные составы мошенничества в сфере компьютерной информации. При рассмотрении данных вопросов было установлено, что способами совершения преступления, предусмотренными ст. 159.6 УК РФ являются — ввод, блокирование, модификация и удаление компьютерной информации, либо иное вмешательство. Фактически можно говорить о том, что здесь употребляется терминология составов преступлений, предусмотренных статьями 272-274 УК РФ.

Диспозиция статьи 159.6 УК РФ является бланкетной, и, чтобы раскрыть в полной мере терминологию, используемую в ней, необходимо обратиться к иным нормативным актам. Тем не менее, даже в таком случае в законодательстве не всегда возможно найти, что понимается под тем или иным термином.

Одной из проблем, связанной с терминологией, является использование термина «удаление» информации. Как было обозначено в работе, формулировка, которая установлена в статье272 УК РФ, является более конкретной и определенной, поскольку в ней используется термин «уничтожение» компьютерной информации, что также было бы целесообразней для использования ее в диспозиции статьи 159.6 УК РФ вместо термина «удаление компьютерной информации».

Помочь преодолеть данную ситуацию способствовали бы разъяснения Пленума Верховного Суда РФ, а также введение определенного ограничения в понимание термина «иное вмешательство» путем применения иной законодательной формулировки.

Одной из характерных особенностей квалифицированных составов мошенничества в сфере компьютерной информации является признание крупным и особо крупным размером, установленным для преступлений, предусмотренных статьей 159.6 УК РФ размера ущерба в шесть раз больше, чем того, который предусмотрен для статьи 159 УК РФ.

Еще одной особенностью квалицированных составов мошенничества в сфере компьютерной информации являются менее строгие размеры санкций, установленных для данных составов в соотношении с «классическим» мошенничеством и смежными составами. В качестве возможного варианта преодоления данной проблемы видим необходимость увеличения размера санкций за мошенничество в сфере компьютерной информации, что позволит минимизировать необоснованность смягчения уголовной ответственности за преступление, предусмотренное ст. 159.6 УК РФ.

В главе второй данного исследования рассмотрены вопросы отграничения состава преступления, предусмотренного статьей 159.6 УК РФ от смежных составов, в частности от статьи 159 УК РФ, а также статей 272-274 УК РФ.

При рассмотрении данной главы был установлен ряд особенностей. Обозначим некоторые из них. Для квалификации преступлений важное значение имеют особые, специфические признаки объективной стороны, а именно — способ совершения преступления. При проведении анализа статей 159 и 159.6 УК РФ были выявлены несовпадения в части признаков объективной стороны этих составов. Диспозиция статьи 159.6 УК РФ не предусматривает такие способы совершения преступления как обман и злоупотребление доверием. Исходя из формулировки диспозиции, можно установить, что мошенничество в сфере компьютерной информации является самостоятельной формой хищения и имеет специфический способ хищения, отличный от других форм хищения. Объективная сторона составов преступлений статей 159 и 159.6 УК РФ не совпадает. В таком случае, вывод будет следующим — данные нормы не находятся в соотношении общей и специальной. В целом можно говорить о том, что статья 159.6 УК РФ имеет основное юридическое разграничение с «классическим» мошенничеством в способе совершения хищения имущества. В связи с изложенным считаем, что сформулировать название преступления, предусмотренного ст. 159.6 УК РФ стоит как «Хищение чужого имущества с применением средств компьютерной техники».

Что касается санкций, то здесь можно выделить следующее. Наказание за неквалифицированный состав преступления в специальном виде мошенничества остается более мягким по сравнению с «классическим» мошенничеством. Это позволяет говорить о некоторой необоснованности смягчения уголовной ответственности за преступление, предусмотренное ч. 1 ст. 159.6 УК РФ. В ч. 4 ст. 159.6 УК РФ изменено понимание особо квалифицирующего признака — особого крупного размера, в связи с чем, к сожалению, можно говорить о том, что это позволило улучшить положение лиц, совершивших мошенничество в сфере компьютерной информации.

При отграничении состава преступления, предусмотренного статьей 159.6 УК РФ от статей, предусмотренных главой 28 УК РФ, устанавливающих ответственность за совершение преступлений в сфере компьютерной информации, было выявлено следующее. Основной отличительной особенностью объективной стороны преступления, предусмотренного статьей 272 УК РФ от объективной стороны статьи 159.6 УК РФ, является то, что исходя из смысла диспозиции статьи 272 УК РФ блокирование, уничтожение, копирование и модификация компьютерной информации являются не способом совершения преступления, а обязательными прямыми последствиями совершенного неправомерного доступа к компьютерной информации. С субъективной стороны преступления, предусмотренные статьями 272 УК РФ и 159.6 УК РФ, отличаются по направленности умысла. Что касается вопроса санкций, назначаемых за совершение данных преступлений, то можно отметить следующее. Санкция, установленная ч. 1 ст. 159.6 УК РФ является менее строгой по отношению к санкциям, установленным в ч. 1 и 2 ст. 272 УК РФ. Также следует отметить, что при квалификации состава, предусмотренного ст. 159.6 УК РФ, необходимо обратиться к Примечанию 1 ст. 272 УК РФ в целях раскрытия и правильного толкования термина «компьютерная информация».

Основным отличием статьи 159.6 УК РФ от статьи 273 УК РФ является способ совершения преступления. Так, способом совершения преступления для преступления, предусмотренного статьей 273 УК РФ, является создание, распространение или использование компьютерных программ или иной компьютерной информации. Уничтожение, блокирование, модификация либо копирование компьютерной информации, выступающие в качестве способа совершения преступления, предусмотренного статьей 159.6 УК РФ, а также нейтрализация средств защиты компьютерной информации, выступают здесь в качестве последствий совершенного виновным лицом преступного деяния, но не в качестве способа совершения преступления.

При отграничении мошенничества в сфере компьютерной информации было выявлено следующее. В качестве обязательного признака для преступления, предусмотренного статьей 274 УК РФ, выступает существенный вред, возникающий вследствие причинения виновным лицом крупного ущерба владельцу ЭВМ, либо пользователю, или же третьим лицам.

Одним из проблемных моментов является то, что все новые нормы мошенничества (в том числе — мошенничество в сфере компьютерной информации) являются бланкетными. В этих нормах не определяются все признаки этих видов преступлений либо дефиниции отсутствующих признаков сформированы в других нормативных актах.

Следует также обозначить тот факт, что в настоящее время в уголовном законодательстве не существует единого термина для обозначения преступлений с использованием компьютерной техники и/ или компьютерных сетей. Тем не менее рядом федеральных законов были внесены дополнения в части внесения в них официального понятия — «преступления, совершаемые с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет». Предпринятая законодательная инициатива позволяет уголовному законодательству идти дальше и иметь развитие в понимании преступлений с использованием компьютерных технологий. Более подробно этот вопрос изложен в работе.

Правоприменительная практика по делам о преступлениях, предусматривающих ответственность за мошенничество в сфере компьютерной информации, крайне невелика. Сложности с установлением наличия в совершенных лицом деяниях всех признаков состава преступления, предусмотренного статьей 159.6 УК РФ возникают в отношении субъекта преступления ввиду его анонимности; объективной стороны — ввиду использования лицом для совершения преступления компьютерных технологий; с точки зрения субъективной стороны — ввиду возникающих сложностей при установлении формы вины, цели и мотива совершения преступления.

Еще одним проблемным моментом является использование в формулировке диспозиции статьи 159.6 УК РФ понятий, требующих обращения к иным нормативным актам в целях их раскрытия. В ряде случаев при отсутствии законодательного регулирования данного вопроса последствием является более широкое или более узкое толкование таких понятий (например, «иное вмешательство»).

В третьей главе исследования рассмотрены правовые и криминалистические проблемы расследования мошенничества в сфере компьютерной информации.

Расследование, равно как и предупреждение мошенничества в сфере компьютерной информации, представляет собой комплексную проблему. Решение ее требует особых специфических знаний, находящихся на границе знаний высоких технологий и юриспруденции. В ходе рассмотрения задач, установленных для данной главы, был проведен анализ и обобщение судебной и следственной практики, в результате чего были выявлены и определены сложности, возникающие при расследовании мошенничества в сфере компьютерной информации. К числу наиболее значимых можно отнести: использование удаленного доступа к компьютерной информации в качестве способа совершения преступления; присутствие специалиста при проведении допроса может двояко сказаться на его результатах и имеет определенные негативные последствия; низкий уровень взаимодействия следствия с оперативными службами; отсутствие методики раскрытия и расследования мошенничества с использованием компьютерной информации, способной оказать значительное влияние на качество раскрытия и расследования данных преступлений. Таким образом, считаем, что в настоящее время существует необходимость разработки методик с учетом последних достижений в области криминалистики, изменений уголовного и уголовно-процессуального законодательства, а также обязательным содержанием в них научно обоснованных криминалистических рекомендаций относительно методики раскрытия, расследования и судебного разбирательства таких преступлений. В целях повышения качества расследования и увеличения раскрываемости данной категории преступлений также необходима разработка особой криминалистической теории, методов и методик, способствующих качественному собиранию, анализу и впоследствии — использованию криминалистически значимой информации.

В заключении отметим, что разрешение существующих проблем требуют всестороннего и компетентного обсуждения с привлечением широкого круга лиц. В данном случае нельзя обойтись без привлечения специалистов в области права, высоких технологий, чтобы как можно более точно переложить общие принципы и подходы борьбы с мошенничеством в сфере компьютерной информации на язык уголовного закона, при этом сохраняя его целостность, системность и фундаментальные положения. Если в полном объеме не продумывать законодательные шаги, то в таком случае они будут способствовать, как в настоящее время способствуют, появлению в уголовном законодательстве еще целого ряда так называемых «мертвых» норм, которые способны не исправить существующую ситуацию, но и усугубить ее.

Список литературы

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 30.12.2015) // Собрание законодательства РФ. 17.06.1996. № 25. ст. 2954.

. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 07.03.2017) // Ведомости Федерального Собрания РФ, 01.01.2002, № 1, ст. 1.

. Федеральный закон от 27.07.2006 № 149-ФЗ об информации, информационных технологиях и о защите информации // Российская газета. № 165, 29.07.2006.

. Федеральный закон от 27.07.2010 N 224-ФЗ (ред. от 21.07.2014) О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации // Российская газета, № 168, 30.07.2010

. Федеральный закон от 20.07.2011 № 250-ФЗ О внесении изменений в отдельные законодательные акты Российской Федерации // Российская газета, № 161, 26.07.2011

. Федеральный закон от 28.07.2012 № 143-ФЗ О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации // Российская газета, № 174, 01.08.2012

. Распоряжение Президента РФ от 22.03.2008 № 144-рп О признании утратившим силу распоряжения Президента Российской Федерации от 15 ноября 2005 г. № 557-рп «О подписании Конвенции о киберпреступности»

. Постановление Пленума Верховного Суда РФ от 27.12.2007 № 51

О судебной практике по делам о мошенничестве, присвоении и растрате // Российская газета. № 4. 12.01.2008

|  |
| --- |
| [Вернуться в библиотеку по экономике и праву: учебники, дипломы, диссертации](http://учебники.информ2000.рф/index.shtml)  [Рерайт текстов и уникализация 90 %](http://учебники.информ2000.рф/rerait-diplom.shtml)  [Написание по заказу контрольных, дипломов, диссертаций. . .](http://учебники.информ2000.рф/napisat-diplom.shtml) |

|  |  |
| --- | --- |
| [**КНИЖНЫЙ МАГАЗИН**](http://учебники.информ2000.рф/chitai.shtml) |  |

|  |  |
| --- | --- |
| [**ТОВАРЫ для ХУДОЖНИКОВ и ДИЗАЙНЕРОВ**](http://учебники.информ2000.рф/kar.shtml) |  |

|  |  |
| --- | --- |
| [**АУДИОЛЕКЦИИ**](http://учебники.информ2000.рф/lectr.shtml) |  |

|  |  |
| --- | --- |
| [**IT-специалисты: ПОВЫШЕНИЕ КВАЛИФИКАЦИИ**](http://учебники.информ2000.рф/otu.shtml) |  |

|  |  |
| --- | --- |
| [**ФИТНЕС на ДОМУ**](http://учебники.информ2000.рф/fit1.shtml) |  |