**Министерство образования и науки Российской Федерации**
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**
**(ФГБОУ ВО «АмГУ»)**

Факультет юридический
Кафедра уголовного права
Направление подготовки 40.03.01 – Юриспруденция

ДОПУСТИТЬ К ЗАЩИТЕ
Зав. кафедрой
_____ Т.Б. Чердакова
«_____»_____2017 г.

# БАКАЛАВРСКАЯ РАБОТА

на тему: Уголовная ответственность за мошенничество в сфере компьютерной информации: проблемы теории и правоприменительной практики

Исполнитель

студент группы 321-сб 5 _____ К. Ю. Лапина

(подпись, дата)

Руководитель

доцент, канд. юр. наук _____ Т.Б. Чердакова

(подпись, дата)

Нормоконтроль _____ О.В. Громова

(подпись, дата)

Благовещенск 2017

**Министерство образования и науки Российской Федерации**
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**
**(ФГБОУ ВО «АмГУ»)**

Факультет: юридический
Кафедра: уголовного права

УТВЕРЖДАЮ
Зав. кафедрой
_____Т.Б. Чердакова

«_____»_____ 2016 г,

**З А Д А Н И Е**

К выпускной квалификационной работе студента Лапиной Кристины Юрьевны.
1. Тема выпускной квалификационной работы: Уголовная ответственность за мошенничество в сфере компьютерной информации: проблемы теории и правоприменительной практики ( утверждена приказом от 10.01.2017 года № 04 – уч.)
2. Срок сдачи студентом законченной работы: 23.01.2017.
3. Исходные данные к выпускной квалификационной работе: Уголовный кодекс Российской Федерации, Уголовно-процессуальный кодекс Российской Федерации, материалы судебной практики, Федеральный закон от 29.11.2012 № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации».
4. Содержание выпускной квалификационной работы (перечень подлежащих разработке вопросов): 1.Теоретические аспекты мошенничества в российском уголовном законодательстве, 2. Проблемы квалификации мошенничества в сфере компьютерной информации, 3. Проблемы правоприменительной практики мошенничества в сфере компьютерной информации.
5. Перечень материалов приложения: (наличие чертежей, таблиц, графиков, схем, программных продуктов, иллюстративного материала и т.п.): Приложение А – Анкета.
Дата выдачи задания: 01.08.2016.
Руководитель выпускной квалификационной работы: Чердакова Татьяна Борисовна, доцент, кандидат юридических наук.
Задание принял к исполнению: 01.08.2016 _____
(подпись студента)

# РЕФЕРАТ

Бакалаврская работа содержит 71 с., 1 приложение, 51 источник.

МОШЕННИЧЕСТВО, ИНФОРМАЦИЯ, КИБЕРПРЕСТУПЛЕНИЕ, ОБМАН, ЗЛОУПОТРЕБЛЕНИЕ ДОВЕРИЕМ, ХИЩЕНИЕ, ПРЕСТУПЛЕНИЯ ПРОТИВ СОБСТВЕННОСТИ, УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ, УЩЕРБ, МОШЕННИЧЕСТВО В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

В данной работе рассматриваются проблемы квалификации мошенничества в сфере компьютерной информации. Объектом исследования являются уголовная ответственность за мошенничество в сфере компьютерной информации. Предметом исследования выступают проблемы, возникающие у судов и правоохранительных органов в процессе привлечения виновных лиц к уголовной ответственности за мошенничество в сфере компьютерной информации. Цель работы заключается в изучении нового состава преступления - мошенничества в сфере компьютерной информации. В процессе исследования перед автором работы стояли такие задачи как, изучение теоретических аспектов мошенничества, рассмотрение его новых составов, рассмотрение и изучение проблем квалификации мошенничество в сфере компьютерной информации, анализ судебной практики рассмотрения уголовных дел о мошенничестве в сфере компьютерной информации, выявление проблем квалификации мошенничества в сфере компьютерной информации, возникающих у сотрудников правоохранительных органов в ходе расследования.

СОДЕРЖАНИЕ

# ВВЕДЕНИЕ

Преступления против собственности являются наиболее распространенным видом преступного посягательства в России, которые наносят огромный урон ее гражданам. Практически каждому человеку в нашей стране так или иначе приходилось сталкиваться с преступными посягательствами такого рода. Мошенничество в данной категории преступлений занимает особое место, так как с каждым годом количество мошеннических посягательств стремительно увеличивается. Более того, данные преступления по своим негативным тенденциям на много опережают в этом плане кражи и грабежи.

Такое преступление, как мошенничество, известно российскому обществу еще со времен Древней Руси и в настоящее время уже успело проникнуть во многие сферы жизни общества и государства. Кроме того данный вид преступного посягательства успешно адаптируется к изменяющимся условиям рынка. А с развитием науки и внедрением в повседневную жизнь новых информационных технологий оно приобрело интеллектуальный оттенок. Ввиду того, что мошенничество, как правило, распознается потерпевшими не сразу, а лишь по прошествии определенного времени, то правоохранительные органы не могут оперативно реагировать на поступившие от граждан заявления и как следствие, данный факт является причиной низкой раскрываемости таких преступлений. Кроме того, значительный имущественныйвред, который причиняется гражданам и юридическимлицам, усовершенствование способов совершения данного преступного посягательства достаточно сильно усугубляет ситуацию по привлечению виновных к наказанию и возмещению потерпевшим ущерба. Часто мошенники совершают преступные посягательства под видом организационно-правовых форм, которые не запрещены законом, используют поддельные документы и банковские карты, а факты мошенничества представляют какразличные сделки гражданско-правового характера. Это так жеявляется значительной преградой при расследовании таких преступлений.

Более того, в последнее время появились новые виды мошенничества, та-

кие как мошенничество с использованием компьютеров, поддельных кредитных карт и банковских авизо, связанные с созданиемфинансовых пирамид, фиктивных инвестиционныхфондов и так далее. За появлением новых способов мошенничества последовала реакция законодателя в виде выделения в УК РФ специальныхсоставов мошенничества.

Актуальность темы данной работы состоит в том, что в условиях развитияобщества, совершенствования компьютерных и информационных технологий, появление огромного количества социальных сетей и неограниченного доступа к ним граждан из самых разных слоев населения, у преступников появляются новые возможности для совершения преступлений путем злоупотребления доверием. На сегодняшний день многие из таких способов мошенничества не достаточно изучены специалистами, поэтому и процент раскрываемости данных преступлений достаточно низок, а процесс расследования затрудняется отсутствием у оперативно- розыскных подразделений правоохранительных органов необходимого современного оборудования и опыта.

Цель бакалаврской работы заключается в изучении нового состава мошенничества в сфере компьютерной информации.

В процессе достижения главной цели работы предусматривается решение ряда конкретных задач:

- изучение теоретических аспектов мошенничества в российском уголовном праве;

- рассмотрение новых составов мошенничества в российском уголовном законодательстве;

- рассмотрение и изучение проблем квалификации одного из новых составов мошенничества – мошенничество в сфере компьютерной информации;

- анализ судебной практики рассмотрения уголовных дел о мошенничестве в сфере компьютерной информации;

- выявление проблем квалификации мошенничества в сфере компьютерной информации, возникающих у сотрудников правоохранительных оганов в ходе расследования.

Информационной методологической базой дипломной работы являются учебные пособия, работы ведущих отечественных ученых в исследуемой области, так же статистические материалы, аналитические статьи отраслевых журналов и интернет – ресурсы.

# 1 ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ МОШЕННИЧЕСТВА В РОССИЙСКОМ УГОЛОВНОМ ПРАВЕ

## 1.1 Понятие и признаки мошенничества в российском уголовном праве

В Уголовном Кодексе Российской Федерации мошенничество определяется как хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.[1] Главное отличие мошенничества от иных преступлений против собственности является то, что потерпевшее лицо будучи обманутым добровольно передает свое имущество преступнику, который злоупотребляя доверием жертвы вводит ее в заблуждение.

В ст. 159 УК РФ законодатель определил ответственность за совершение мошеннических действий.

Предметом мошенничества может быть как чужое имущество, так и право на него. Например, право пользования нежилыми помещениями, земельными участками и другое. В этом и заключается специфичность данной формы хищения. Объективная сторона мошенничества выражается в том, что хищении чужого имущества или приобретении права на него осуществляется обязательно путем обмана или злоупотребления доверием. Обман в данном случае является способом хищения имущества. В науке уголовного права различают активный и пассивный обман.

Активный обман имеет место быть когда мошенник умышленно сообщает потерпевшему заведомо ложныесведенияили каким-либо образом укрывает истинные факты от него, либовводит владельца имущества или другое заинтересованное лицо в заблуждение предоставляя, например поддельный товар или используя какие – либо приемы для совершения обмана при расчете за товары или услуги. При пассивном обмане мошенник утаивает о юридически значимых обстоятельствах, которые он обязан был сообщить потерпевшему. Напри-

[1]Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (в ред. от 07 февраля 2017 г.) // Собрание законодательства РФ. 1996. № 25. С. 4578-4689.

мер, о недостатках продаваемого товара, его стоимости или же об отсутствии у преступника полномочий для его передачи другим лицам. В результате данных действий потерпевший заблуждается относительно наличия у него законных оснований для передачи виновному имущества или права на него.[2]

В случаях, когда виновный использует обманне как способ хищения имущества, а как средстводля более легкого доступа к нему, действия преступника не будут квалифицироваться как мошенничество.

Еще одним способом совершения мошенничества является злоупотребление доверием потерпевшего. Согласно п. 3 постановления Пленума Верховного Суда РФ от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» злоупотребление доверием заключается в использовании с корыстной целью доверительных отношений с владельцем имущества или иным лицом, уполномоченным принимать решения о передаче этого имущества третьим лицам.[3] Доверииможет быть обусловлено различными обстоятельствами, например служебным положением лица либоличными или родственными отношениями лица с потерпевшим. Примером указанного способа мошенничества является преднамеренное неисполнение принятых виновным на себя обязательств (например, получение физическим лицом кредита, аванса завыполнение работ или оказание услуг, предоплаты запоставку товара без действительного намерениявозвращать долг или иным образом исполнять свои обязательства). В случаях с злоупотреблением доверия, как и при обмане владелец имущества, будучи введенным в заблуждение, добровольно передает его преступнику, думая, что действует в своихинтересах. Необходимо отметить, что если имущество было доверено, а не передано преступнику, то данный случай не будет являться мошенничеством. Довольно часто при совершении мошеннических действий преступник использует поддельные документы. При этом, если данный документ был подделан иным лицом, то преступление

[2]Александрова И.А. Новое уголовное законодательство о мошенничестве // Юридическая наука и практика. Вестник Нижегородской академии МВД России. 2013. № 21. С. 54- 62.

[3]Постановление Пленума Верховного суда РФ от 27 декабря 2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» (в ред. от 29 ноября 2012 г.) // Российская газета. 2008. 15 авг.

так же будет содержать элемент мошенничества и дополнительнаяквалификация по ч. 3 ст. 327 УК РФ в таком случае не требуется. Однако в соответствии с п. 6 постановления Пленума Верховного СудаРФ от 27 декабря 2007 г. № 51 «О судебной практикепо делам о мошенничестве, присвоении и растрате» хищение чужого имущества или приобретение правана него путем обмана или злоупотребления доверием,совершенные с использованием подделанного этимлицом официального документа, предоставляющегоправа или освобождающего от обязанностей, квалифицируется как совокупность преступлений, предусмотренных ч. 1 ст. 327 УК РФ и соответствующей частью ст. 159 УК РФ. Если мошенник в силу каких-либо обстоятельств, не воспользовался данным документом, то преступное деяние необходимо квалифицировать по ч. 1 ст. 30 и соответствующей части ст. 159, а также по ч. 1 ст. 327 УК РФ.[4]

Мошенничество считается оконченным с момента передачи имущества, в результате обмана или злоупотребления доверием, преступнику или другим лицам, получившим вместе с этим возможность распоряжаться им. Если итогом мошеннических действий сталоприобретение права на чужое имущество, то в данном случае преступление будет считаться оконченным с момента возникновения у мошенниказаконного, юридически оформленного права распоряжатьсяим. Например, с момента регистрации права собственности на недвижимость или других имущественных прав, подлежащих такой регистрации.

К составу мошенничества так же относятся случаи, когда лицо создает коммерческую организацию, но при этомне намеревается осуществлять предпринимательскую деятельность, а использует ее для хищения чужого имущества. Такие случаи не требуют дополнительной квалификации по ст. 173 УК РФ – осуществление незаконной предпринимательской деятельности. Не подлежат дополнительно квалификации по ст. 171 УК РФ и случаи, когдаизготовление и сбытфальсифицированных товаров сопряжен с обманом потребителей относительно их качества и иных характеристик. Однако сами действия по изготовле-

[4]Постановление Пленума Верховного суда РФ от 27 декабря 2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» (в ред. от 29 ноября 2012 г.) // Российская газета. 2008. 15 авг.

нию и реализации товаров, не отвечающих требованиям безопасности жизни и здоровья людей, составляют совокупность таких преступлений как мошенничество и преступления, предусмотренные ст. 238 УК РФ. Получение при помощи обмана и чужих личных документов социальных выплат, денежных переводов, банковских вкладов так же надлежит квалифицировать как мошенничество согласно п. 11 Постановления Пленума.[5]

Основными характеристиками субъективной стороны мошенничества является прямой умысел и корыстная цель посягательства. Субъектом мошенничества является достигшее шестнадцатилетнего возраста лицо. Мошеннические действия, совершенные при квалифицирующих и особо квалифицирующих обстоятельствах ч.ч. 2-7 ст. 159 УК РФ наиболее опасные. Квалифицирующим признаком по ч. 2 ст. 159 УК РФ является совершение мошенничества группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину.

Хищением, совершенным по предварительному сговору группой лиц, является хищение, участие в котором принимали двое и более лиц, заранее договорившихся о совместном его совершении согласно ч. 2 ст. 35 УК РФ.

Как правило, сговор между виновными должен быть достигнут до совершения мошеннических действий, то есть на стадии приготовления к преступлению. Сговор, возникший в момент осуществления преступных действий, которые составляют объективную сторону хищения, не является предварительным.[6]

Действия всех лиц, участвующих в совершении преступления, должны содержать в себе признаки как объективной, так и субъективной стороны состава мошенничества. В связи с этим не образуют рассматриваемого признака действия организатора, подстрекателя, пособника. В таких случаях ответственность наступает по ст. 159 УК РФ со ссылкой на ст. 33 УК РФ («Виды соучастников преступления»). Судебная практика квалифицирует преступление как со-

[5]Постановление Пленума Верховного суда РФ от 27 декабря 2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» (в ред. от 29 ноября 2012 г.) // Российская газета.2008. 15 авг.
[6]Андреев Б.В. Расследование преступлений в сфере компьютерной информации. М.: МАИК «Наука / Интерпериодика». 2015. С. 527.

вершенное группой лиц только при наличии как минимум двух соисполнителей, каждый из которых выполняет часть объективной стороны преступления.[7] Содействие совершению преступления лицом, непосредственно не участвовавшим в хищении, надлежит квалифицировать как соучастие со ссылкой на ст. 33 УК РФ.

Мошенничество, совершенное несколькими лицами без предварительного сговора, следует квалифицировать по ч. 1 ст. 159 УК РФ. Но совершение преступления группой лиц может признаваться судом обстоятельством, отягчающим наказание (п. «в» ч. 1 ст.63 УК РФ).

В случае совершения мошенничества спривлечением лиц, не подлежащих уголовной ответственности в силу возраста, невменяемости или других обстоятельств, действия мошенника, при отсутствии иныхквалифицирующих признаков, следует квалифицировать по ч. 1 ст. 159 УК РФ так как он будет являться исполнителем преступления. Таким же образом будут квалифицироватьсядействия лица, которое при организации преступления склонило к его совершению лицо не подлежащего уголовной ответственности. Действия указанных лиц могут дополнительно квалифицироваться по ст. 150 УК РФ если на то есть необходимые основания. [8]

Потерпевшим от мошенничества, совершенного с причинением значительного ущерба может быть лишь физическое лицо.

Часть 3 ст. 159 УК РФ предусматривает уголовную ответственность за мошенничество, совершенное лицом с использованием своего служебного положения, а равно в крупном размере. Субъектом преступления в данном случае, будет лицо, выполняющее управленческие функции в коммерческой или иной организации, а так же должностное лицо, государственный или муниципальный служащий, не являющийся должностным лицом или лицо, выполняющее управленческие функции в коммерческой или иной организации, которое ис-

[7]Журавлев М.А. Актуальные вопросы судебной практики по уголовным делам о мошенничестве // Уголовное право. 2008. № 2. С.95-101.

[8]Постановление Пленума Верховного суда РФ от 27 декабря 2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» (в ред. от 29 ноября 2012 г.) // Российская газета.2008. 15 авг.

пользует свое служебное положениедля незаконного завладения чужим имуществом или приобретения права на него.[9] В случаях, когда должностное лицо, совершает какие-либо действия в интересах другого лица и при этом получает от последнего вознаграждение, то его действия должны квалифицироваться по ст. 290 УК РФ, как получение взятки, помимо ответственности за мошенничество, а аналогичные действия лица, выполняющего управленческие функции в коммерческой или иной организации, как коммерческий подкуп по ч. 3 или ч. 4 ст. 204 УК РФ.

При совершении нескольких преступных посягательств с хищением чужого имущества преступление следует квалифицировать как совершенное в крупных размерах, если общая стоимость такого имущества превышает двести пятьдесят тысяч рублей. Совершены такие хищения должныбыть единым способом и при обстоятельствах, указывающих на умысел мошенника совершить хищение в крупных размерах. При квалификации хищения, совершенного несколькими лицами, следует исходить из стоимости похищенного всеми участниками группы. Когда определяется размер ущерба, необходимо учитывать фактическую стоимость всего похищенного имущества. Если есть такая необходимость, то для определениястоимости имущества возможно проведение соответствующей экспертизы.

Если мошенничество совершенное в крупном размере причиняет значительный ущерб потерпевшему, то действия мошенника квалифицируется по ч. 3 ст. 159 УК РФ, однако в описательной части приговора должен быть отмечен данный факт.

В ч. 4 ст. 159 УК РФ в качестве особо квалифицирующего признака мошенничества выступает совершение преступного посягательства организованной группой лиц или в особо крупном размере. Такой вид мошенничества наиболее опасен, так как совершается всоставе группы характеризующейся устойчивостью, и в составе которой, как правило, имеется организатор. Кроме того,

[9]Колоколов Н.А. Мошенничество: эффективность уголовно-правового запрета // Уголовный процесс. 2012. № 5. С. 115-125.

лица, входящие в состав данной группы, действуют согласноранее составленного плана, в котором четко распределены функции между всеми членами группы. Все участники, вне зависимости от их роли в совершении мошенничества привлекаются к ответственности как соисполнители без ссылки на ст. 33 УК РФ. Если мошенник являетсяподстрекателем другого лица или целой группы лиц к созданию организованной группы для совершения мошеннических действий, но самогоучастия в подборе ее участников, планировании и подготовке преступления не принимает, то его действия подлежат квалификациипо ч. 4 ст. 33 УК РФ, как соучастие в совершении организованной группой.

Федеральным законом от 29.07.2016 № 323- ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации по вопросам совершенствования оснований и порядка освобождения от уголовной ответственности» были внесены изменения в ст. 159 УК РФ. Ст 9 данного закона состав ст. 159 УК РФ дополнили ч.ч. 5, 6, 7.

Квалифицирующим признаком в вышеупомянутых частях ст. 159 УК РФ является предпринимательская деятельность. Так ч. 5 ст. 159 УК РФ предусматривает уголовную ответственность за мошенничество сопряженное с преднамеренным неисполнением договорных обязательств в сфере предпринимательской деятельности, если это деяние повлекло причинение значительного ущерба. Частью 6 ст. 159 УК РФ уголовному наказанию подлежит деяние, предусмотренное частью пятой настоящей статьи, совершенное в крупном размере, а частью 7 - деяние, предусмотренное частью пятой настоящей статьи, совершенное в особо крупном размере. При этом значительным ущербом в части пятой ст. 159 УК РФ признается ущерб в сумме, составляющей не менее десяти тысяч рублей.Крупным размером в части шестой настоящей статьи признается стоимость имущества, превышающая три миллиона рублей.Особо крупным размером в части седьмой настоящей статьи признается стоимость имущества, превышающая двенадцать миллионов рублей.[10]

[10]Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (в ред. от 07 февраля 2017 г.) // Собрание законодательства РФ. 1996. № 25. С. 4123-4256.

Кроме того, действие частей пятой - седьмой ст. 159 УК РФ распространяется на те случаи, когда речь идет о преднамеренном неисполнениобязательств по различным договорам в сфере предпринимательской деятельности, когда договора заключаются междуиндивидуальными предпринимателями и (или) юридические лица.

### 1.2 Новые составы мошенничества в российском законодательстве

Федеральным законом РФ «О внесении изменений в Уголовный кодексРоссийской Федерации и отдельные законодательный акты Российской Федерации» от 29 ноября 2012 г. № 207 – ФЗ Уголовный кодекс РФ был дополнен шестью новыми составами преступлений, предусматривающими ответственность за различные виды мошеннических действий:

- мошенничество в сфере кредитования (ст. 159.1);
- мошенничество при получении выплат (ст. 159.2);
- мошенничество с использованием платежных карт (ст. 159.3);
- мошенничество в сфере предпринимательской деятельности (ст.159.4);
- мошенничество в сфере страхования (ст. 159.5);
- мошенничество в сфере компьютерной информации (ст. 159.6).[11]

Как полагал законодатель, такое выделение отдельных видов мошенничества всамостоятельные составы должно было способствовать повышению эффективности борьбы с данным преступным деянием.

Важно отметить, что новые статьи УК РФ 159.1-159.6 являются специальными по отношению к ст. 159. Согласно правилу, определенному в ч. 3 ст. 17 УК РФ, в случаях, когда ответственность за преступление предусмотрена как общей, так и специальной нормами, то совокупность преступлений отсутствует, а ответственность наступает по специальной норме. Поэтому если лицо совершит, например, мошенничество с использованием платежных карт, тоего действия должны быть квалифицированы только по ст. 159.3 УК РФ. Дополнительной квалификации данного деяния по ст. 159 УК РФ не подлежат. Однако,

[11]Федеральный закон от 29 ноября 2012 г. № 207- ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» (в ред. от 03 июля 2016 г.) // Собрание законодательства РФ. 2012. № 49. С. 3524-3782.

если в действиях лица будут усмотреныпризнаки двух и более специальных составов мошенничества, то каким бы ни было их сочетание, его действия будут квалифицироваться по совокупность преступлений.

Исходя из диспозиций специальных составов мошенничества, их объективной стороной является совершение преступных действийпутем обмана или злоупотребления доверием, как предусмотрено и ст. 159 УК РФ. В каждой из новых статей, законодатель четко определилпредмет преступления, который, не всегда совпадает с предметом преступления описанном в ст. 159 УК РФ. То есть предметом специальных составов мошенничества не всегда будет чужое имущество или право на него. В ст. 159. 1 УК РФ предметом преступления выступают денежные средства, в ст. 159.2 УК РФ - денежные средства и иное имущество, в ст. 159.3 УК РФ и в ст. 159.5 УК РФ – только чужое имущество. Что касаетсяст. 159.6 УК РФ, то в данном составе описание предмета преступления абсолютно идентично тому, что закрепленов ст. 159 УК РФ.[12]

Для анализа специальных составов мошенничества используются традиционные для данного преступного деяния квалифицирующие признаки:

– группа лиц по предварительному сговору – данный признак характерен для: ч. 2 ст. 159.1, ч. 2 ст. 159.2, ч. 2 ст. 159.3, ч. 2 ст. 159.5, ч. 2 ст. 159.6;

– причинение значительного ущербагражданину - характерный признак ч. 2 ст. 159.3, ч. 2 ст. 159.5, ч. 2 ст. 159.6;

– использование служебного положения – характеризует ч. 3 ст. 159.1, ч. 3 ст. 159.2, ч. 3 ст. 159.3,ч. 3 ст. 159.5, ч. 3 ст. 159.6;

– крупный размер - ч. 3 ст. 159.1, ч. 3 ст.159.3, ч. 3 ст. 159.5, ч. 3 ст. 159.6;

– организованная группа - ч. 4 ст. 159.1, ч. 4 ст. 159.2, ч. 4 ст. 159.3, ч. 4 ст. 159.5, ч. 4 ст. 159.6;

– особо крупный размер - ч. 4 ст. 159.1, ч. 4 ст. 159.2, ч. 4 ст. 159.3, ч. 4 ст. 159.5, ч. 4 ст. 159.6.

В примечании к ст. 159.1 УК РФ применительно к этой статье, а также к

[12]Янин П.С. Специальные виды мошенничества // Законность. 2015. № 8. С. 15-19.

ст.ст. 159.3, 159.5, 159.6 установлена иная стоимость имущества в крупном и особо крупном размере, чем та, которая определена в примечании к ст. 158 УК РФ для статей гл. 21 «Преступления против собственности». Крупным размером признается стоимость имущества, превышающая один миллион пятьсот тысяч рублей, особо крупным – шесть миллионов рублей. В примечании же к ст. 158 крупным размером признается стоимость имущества, превышающая двести пятьдесят тысяч рублей, а особо крупным – один миллион рублей.[13] Таким образом, стоимость имущества для пяти из шести новых составов мошенничества увеличена в шесть раз, что, безусловно, улучшает положение лиц, совершивших преступления, предусмотренные выше обозначенными статьями.

Однако стоимость имущества при причинении значительного ущерба гражданину составляет не менее пяти тысяч рублей, как и в примечании к ст. 158 УК РФ, согласно последним изменениям, внесенным в УК РФ Федеральным законом от 03.07.2016 № 323- ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации по вопросам совершенствования оснований и порядка освобождения от уголовной ответственности».

При установлении значительного ущерб гражданину в статьях главы «Преступления против собственности» принимается во внимание его имущественного положения,однако если фактическая стоимость имущества меньше пяти тысяч рублей, то ущерб значительным не является.

Следует отметить, что нормы, установленные новыми статьями УК РФ, являются бланкетными, так как в них определяются не все признаки предусмотренных ими преступлений и отсутствующие признаки определяются в других (не уголовных) законах и (или) иных нормативных правовых актах. Так ссылаются на другие законы и нормативно - правовые акты ч. 1 ст. 159.2 и ч. 1 ст. 159.5 УК РФ.

Таким образом, для определения составов преступлений, предусмотрен-

[13]Уголовный кодекс Российской Федерации от 13 июня 1996 г. №63-ФЗ (в ред. от 07 февраля 2017 г.) // Собрание законодательства РФ. 1996. № 25. С. 4123-4527.

ных новыми статьями мошенничества, и их признаков необходимо проанализировать и рассмотреть содержания норм как УК РФ, так и иных законов и нормативно - правовых актов.

При сравнении санкций новых статей о мошенничестве 159.1, 159.2, 159.3, 159.5, 159.6 и санкций ст. 159 УК РФ необходимо отметить, что максимальное наказание за мошенничество в особо крупном размере по прежнему составляет десять лет лишения свободы. Однако санкции новых статей за мошеннические действия без отягчающих обстоятельств в отличие от ст. 159 УК РФ не содержат наказание в виде лишения свободы. Уменьшено максимальное наказание по второй и третьей частях ст. 159 УК РФ на один год, соответственно, с пяти лет лишения свободы до четырех и с шести лет лишения свободы до пяти. Данная мера способствовалапереводу преступлений, квалифицируемых по части третьей, из категории тяжких в категорию средней тяжести, что существенно улучшило положение лица, совершившеготакие мошеннические действия. Кроме того, в пяти новых составах, предусматривающих ответственность за мошенничество, санкции первых частей не включают такую меру наказания, как лишение свободы.

В связи с изменениями Уголовного кодекса РФ и появления новых составов о мошенничестве, многие юристы стали говорить о необходимости внесения соответствующих изменений в постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате», а некоторыеученные говорят о создании нового постановлении Пленума Верховного Суда Российской Федерации, которое будет посвящено различным видам мошенничества и проблемам их квалификации.

В общем, анализируя новые составы мошенничества, возможно стоит согласиться с мнениями некоторых криминалистов, которые утверждают, что введенные нормы, по своей сути направлены на смягчение ответственности за мошенничество, совершаемое в отдельных сферах общественной жизни.

Таким образом в данной главе были изучены теоретические аспекты мо-

шенничества в российском уголовном праве, процесс развития законодательства о данном преступлении в России и зарубежных странах, а так же рассмотрены новые специальные составы мошенничества.

Согласно УК РФ мошенничество – это хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. Главными отличительными признаками мошенничества от других имущественных преступлений, являются способы его совершения, а именно обман и злоупотребления доверием, при помощи которых преступник вводит жертву в заблуждение.

Обман как способ хищения чужого имущества может быть активным или пассивным.

Активный обман - это умышленное сообщении ложных сведений либо умолчание об истинных фактах, а также умышленные действиях, направленные на введение владельца имущества или иного лица в заблуждение.

Пассивный обман заключается только в умолчании виновным лицом о юридически значимых фактических обстоятельствах, сообщить которые он был обязан.

Злоупотребление доверием заключается в использовании с корыстной целью доверительных отношений с владельцем имущества или иным лицом, уполномоченным принимать решения о передаче этого имущества третьим лицам.

Мошенничество считается оконченным с момента, когда в результате обмана или злоупотребления доверием чужое имущество поступило в незаконное владение виновного или других лиц, и они получили реальную возможность пользоваться им или распорядиться по своему усмотрению.

Нередко мошеннические действия совершаются с использованием фиктивных документов.

Создание коммерческой организации без намерения осуществлять предпринимательскую деятельность, а преследующее цель хищения чужого имущества, так же может охватываться составом мошенничества.

Субъективная сторона мошенничества характеризуется прямым умыслом и корыстной целью. Субъектом мошенничества является лицо, достигшее 16-летнего возраста.

Квалифицирующим признаком по ч. 2 ст. 159 УК РФ является совершение мошенничества группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину. Потерпевшим от мошенничества, совершенного с причинением значительного ущерба гражданину является лишь физическое лицо.

Часть 3 ст. 159 УК РФ предусматривает уголовную ответственность за мошенничество, совершенное лицом с использованием своего служебного положения, а равно в крупном размере.

В ч. 4 ст. 159 УК РФ в качестве особо квалифицирующего признака называется мошенничество, совершенное организованной группой либо в особо крупном размере.

Квалифицирующим признаком в ч.ч. 5-7 ст. 159 УК РФ является предпринимательская деятельность. Так, ч. 5 ст. 159 УК РФ предусматривает уголовную ответственность за мошенничество сопряженное с преднамеренным неисполнением договорных обязательств в сфере предпринимательской деятельности, если это деяние повлекло причинение значительного ущерба. Частью 6 ст. 159 УК РФ уголовному наказанию подлежит деяние, предусмотренное частью пятой настоящей статьи, совершенное в крупном размере, а частью 7 - деяние, предусмотренное частью пятой настоящей статьи, совершенное в особо крупном размере. При этом значительным ущербом в части пятой статьи 159 УК РФ признается ущерб в сумме, составляющей не менее десяти тысяч рублей.

Федеральным законом РФ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательный акты Российской Федерации» от 29 ноября 2012 г. № 207-ФЗ Уголовный кодекс РФ был дополнен шестью новыми составами преступлений, предусматривающими ответственность за различные виды мошеннических действий:

- мошенничество в сфере кредитования (ст. 159.1);

- мошенничество при получении выплат (ст. 159.2);

- мошенничество с использованием платежных карт (ст. 159.3);

- мошенничество в сфере предпринимательской деятельности (ст.159.4);

- мошенничество в сфере страхования (ст. 159.5);

- мошенничество в сфере компьютерной информации (ст. 159.6).

Данная дифференциация ответственности за мошенничество путем выделения отдельных видов в самостоятельные составы, по мысли законодателя способствует повышению эффективности борьбы с этим видом хищения.

Необходимо отметить, что вновь введенные в УК РФ ст.ст. (1591–1596) являются специальными по отношению к ст. 159. Поэтому, по правилу, закрепленному в ч. 3 ст. 17 УК РФ, если преступление предусмотрено общей и специальной нормами, совокупность преступлений отсутствует и уголовная ответственность наступает по специальной норме.

Из описания диспозиций новых составов мошенничества, их объективная сторона по-прежнему выполняется путем обмана или злоупотребления доверием. В каждой из новых статей, указывается предмет преступления.

В анализируемых статьях используются традиционные для состава мошенничества квалифицирующие признаки:

– группа лиц по предварительному сговору;

– причинение значительного ущерба гражданину;

– использование служебного положения;

– крупный размер;

– организованная группа;

– особо крупный размер.

Следует отметить, что нормы, установленные новыми статьями УК РФ, являются бланкетными, так как в них определяются не все признаки предусмотренных ими преступлений и отсутствующие признаки определяются в других (не уголовных) законах и (или) иных нормативных правовых актах.

Сравнительный анализ санкций ст.ст. 159.1, 159.2, 159.3, 159.5, 159.6 и

санкций ст. 159 УК РФ показывает, что максимальное наказание за мошенничество в особо крупном размере по прежнему составляет десять лет лишения свободы. Однако санкции новых статей за мошеннические действия без отягчающих обстоятельств в отличие от ст. 159 УК РФ не содержат наказание в виде лишения свободы. В целом же, оценивая новые составы мошенничества, следует согласиться свыводом большинства криминологов, что проанализированные нормы, безусловно, направлены на существенное смягчение ответственности за мошенничество, совершаемое в отдельных сферах. Однако их введение было обусловлено развитием общественных и экономических отношений, а так же совершенствованием коммуникационных технических средств.

Несмотря на то, что специальные составы мошенничества были введены законодателем еще в 2012 году, на сегодняшний день существует ряд вопросов и проблем, связанных с их расследованием и квалификацией, которые требуют более детального изучения. В связи с этим в следующей главе данной дипломной работы будет рассмотрены вопросы проблем квалификации одного из специальных составов мошенничества – мошенничество в сфере компьютерной информации.

# 2 ПРОБЛЕМЫ КВАЛИФИКАЦИИ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

## 2.1 Мошенничество в сфере компьютерной информации, как новый состав преступления

Федеральным законом № 207-ФЗ от 29.11.2012 в действующий Уголовный кодекс Российской Федерации включена ст. 159.6 «Мошенничество в сфере компьютерной информации».

Указанное деяние находится в одном ряду с мошенничеством в сфере кредитования, при получении выплат, с использованием платежных карт, в области страхования.

Мошенничество в сфере компьютерной информации является закономерным шагом интеграции российского законодательства о борьбе с компьютерными преступлениями в международное. До настоящего времени основнаядеятельность в указанной сфере осуществлялась в рамках требований ст.ст. 272 - 274 УК РФ, формально подпадающих под положения Европейской Конвенции о киберпреступности, фактически оставляя без внимания вопросы ответственности засовершение преступлений, связанных с использованием компьютерных средств.

Включение указанной статьи в уголовное законодательство способствует конкретизации компьютерных преступлений, наряду с преступлениями в сфере компьютерной информации выделяяпреступления, осуществляемые с использованиемкомпьютерных средств. Однако включение данного состава преступления в уголовное законодательство Российской Федерации порождает также ряд проблем.

Диспозиция ст. 159.6 УК РФ[14] определяет под мошенничеством в сфере компьютерной информации хищение чужого имущества или приобретениеправа на чужое имущество путем ввода, удаления, блокирования, модификации

[14] Уголовный кодекс Российской Федерации от 13 июня 1996 г. №63-ФЗ (в ред. от 07 февраля 2017 г.) // Собрание законодательства РФ. 1996. № 25. С. 4123 – 1527.

компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачикомпьютерной информации или информационно - телекоммуникационных сетей.

Таким образом, формулировка указанного состава преступления, принятая в российскойкриминалистике в полном объеме совпадает с дефиницией, предложенной Конвенцией о киберпреступности, которая в ст. 8 под мошенничеством с использованием компьютерных технологий понимает «лишение другого лица егособственности путем любого ввода, изменения,удаления или блокирования компьютерных данных, либо вмешательства в функционированиекомпьютерной системы, с мошенническим илибесчестным намерением неправомерного извлечения экономической выгоды для себя или для иного лица».[15]

При этом обращает на себя внимание то обстоятельство, что в указанной Конвенции мошенничество с использованием компьютерных технологий,наряду с подлогом с использованием компьютерных технологий составляет раздел преступленийс использованием компьютерных средств. Такимобразом выделена отдельная категория преступлений, где компьютерная информация выступает вкачестве средства совершения преступления. Указанная категория стоит в ряду с преступлениямипротив конфиденциальности, целостности и доступности компьютерных данных и систем; преступлениями, связанными с содержанием данныхи преступлениями в сфере авторских и смежныхправ. При этом создается достаточно целостная картина киберпреступлений, объединяемых родовым объектом и дифференцируемых видовымиобъектами состава преступления.

Положениями п. 166 Резолюции X Конгресса ООН по предупреждению преступности и обращению с правонарушителями, состоявшемся 10 - 17 апреля 2000 года в Вене определено: «если компьютерные данные поддаются идентификации иконтролю по конкретному носителю данных, тос юридической точки

[15]Конвенция совета Европы от 23.11.2001 ETS № 185 «О преступности в сфере компьютерной информации» (в ред. дополнительного протоколом от 28 января 2003 г. ETS № 189) [Электронный ресурс]. URL: http:// www.consultant.ru/. (дата обращения: 15.09.2016).

зрения они могут рассматриваться как единый и ощутимый материальный предмет».

Статья 159.6 УК РФ состоит из четырех частей,первая из которых раскрывает понятие мошенничества в сфере компьютерной информации, 2, 3 и 4 части указанной статьи содержат квалифицированные составы данного преступления по признакам:

- деяния, совершенного группой лиц по предварительному сговору (ч. 2);

- с причинением значительного ущерба гражданину (ч. 2);

- совершения лицом с использованием своего служебного положения (ч. 3);

- совершения в крупном размере (ч. 3);

- совершения организованной группой (ч. 4);

- совершения в особо крупном размере (ч. 4).

Преступление, предусмотренное ч. 1 ст. 159.6 УКРФ является преступлением небольшой степенитяжести, преступления, предусмотренные ч. 2 и 3 ст. 159.6 УК РФ – преступлениями средней тяжести, а преступления, предусмотренные ч. 4 указанной статьи, – отнесены к тяжким.[16]

Анализ указанной статьи позволяет сделать следующие выводы:

- 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;

- объективную сторону мошенничества в сфере компьютерной информации составляет хищение чужого имущества или приобретение права на чужое имущество;

- способом совершения преступления выступает: ввод, удаление, блокирование, модификация компьютерной информации; иное вмешательство в

[16]Гарбатович Д.А. Проблемные аспекты эффективности норм, предусматривающих уголовную ответственность за совершение преступлений в сфере компьютерной информации // Библиотека криминалиста. 2013. № 5 (10). С. 40 - 47.

функционирование средств хранения, обработки или передачи компьютерной информации или информационно - телекоммуникационных сетей;

- субъект – общий, по ч. 3 ст. 159.6 УК РФ – специальный, квалифицирующими признаками выступает совершение преступления группой лиц по предварительному сговору, либо организованной группой;

- субъективная сторона предполагает прямой умысел. Виновный осознает, что завладевает чужим имуществом или правами на него путем ввода, удаления, блокирования, модификации компьютерной информации либо иным вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Понятие компьютерной информации применительно к уголовно-правовым отношениям раскрывается примечанием к ст. 272 УК РФ, согласно которому под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Вопрос о материальности компьютерной информации раскрывается через призму того обстоятельства, что информация представляет собой способ отражения объективной реальности в ее разнообразии форм распространения и изменчивости.

По всей видимости, именно поэтому, все науки,осуществляющие активное использование информации, деликатно обходят стороной вопрос о материальности информации как таковой, категорически настаивая на материальности информации в связи с ее носителем.

Информация существует объективно, но воспринимается всегда субъективно. При этом возникаетвзаимосвязь между информацией и ее материальным носителем. При взаимодействии информациии носителя свойства каждого из них в значительноймере изменяются.

Таким образом, вполне закономерным представляется выделения характеристик информациииименно в ее связи с носителем, что приводит нас кпони-

манию сущности информационного объектаи, далее, к документированной информации.

Информация передается и распространяется только на материальномносителе или с помощью материального носителя и проявляется как «двуединство» информации (ее содержания) и носителя, на котором эта информация (содержание) закреплена.[17]

В том, что касается общественно-опасных последствий данного мошенничества, обращают насебя внимание следующие обстоятельства: поскольку преступление, предусмотренное ст.159.6 УК РФ является преступлением с материальным составом, обязательным условием его совершения выступает хищение чужого имущества илиприобретение права на чужое имущество. При этомвозникает вопрос о том, что конкретно похищенов результате совершения преступления: деньги, информация, права или что-то еще.

Таким образом, особую актуальность приобретает проблема информации как вещи, имущества.

В силу ряда свойств, у информациинет собственника, а только обладатель, что нашлосвое отражение в ряде законов информационнойотрасли права. Применяя понятие информационного объекта, информационной вещи, следуетиметь в виду, что информация, обладая стоимостью, не является имуществом как совокупностьвещей.

Таким образом, вопрос о возможности рассмотрения информационной вещи в качестве предметамошенничества, в настоящее время не может решатьсяоднозначно и нуждается в дальнейшей проработке.

Включение статьи о мошенничестве в сфере компьютерной информации в российское уголовное законодательство, с одной стороны,должно упростить процедуру выявления и расследования преступлений данной категории как на национальном,так и на международном уровне, исключить возможность уголовного преследования граждан Российской Федерации за совершение киберпреступлений на территории других стран и их ответственность позарубежному

[17]Гульбин Ю.А. Преступления в сфере компьютерной информации. М.: Статут, 2007. С. 151.

уголовному законодательству.

С другой стороны, диспозиция ст. 159.6 УК РФ с учетом особенностей российского законодательства должна определять мошенничество с использованием информационно-коммуникационных технологий или компьютерной информации как хищение чужого имущества или приобретение права на чужое имущество путем неправомерных действий, связанных с вводом, удалением, блокированием, модификацией компьютерной информации либо иным неправомерным вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

В то же время, формальное отнесение преступлений данной категории к преступлениям противсобственности порождает правовые коллизии в связи с невозможностью правоохранительных органов ответить на вопросы:

- о собственнике информации;
- о размере ущерба;
- об имущественных характеристиках компьютерной информации;
- о взаимосвязи правомерных действий (ввода, удаления, блокирования, модификации компьютерной информации) и общественно-опасных последствий (хищение чужого имущества или приобретение права на чужое имущество);
- о разграничениях между ст. 159.6 УК РФ исмежными составами преступления и другие.

Таким образом, можно сделать вывод, что в диспозиции данной статьи не учтены особенности правового регулирования информационных отношений, самогопонимания феномена информации, что порождаетсложности в практике привлечения к уголовнойответственности за совершение компьютерногомошенничества.

Для разрешения возникающих проблем представляется необходимым выделение в российском уголовном кодексе раздела, посвященногокомпьютерным преступлениям, куда необходимовключить отдельными главами преступ-

ления в сфере компьютерной информации, преступления с использованием компьютерных технологий, преступления в отношении конфиденциальной информации, намеренно выделяя видовые объекты, что в значительной мере должно способствовать пониманию сущностиданной категории преступлений и возможности правоприменения.

## 2.2 Критерии криминализации мошенничества в сфере компьютерной информации

Криминализация является частью уголовной политики государства. Уголовная политика не может быть бессистемной и произвольной. Она должна иметь прочную научную основу, включающую науку уголовного права и криминологию.

Общественная опасность как социальное свойство преступного деяния является главным основанием криминализации.

Задачей законодателя является своевременное выявление общественно опасных деяний, причиняющих вред личности, обществу и государству, борьбу с которыми целесообразно осуществлять уголовно-правовыми средствами.

Общественную опасность деяния формируют так называемые криминообразующие признаки, в число которых включают традиционно общественно опасные последствия, форму вины, цель, способ (насильственный, групповой, с использованием служебных полномочий, обманный).

В качестве главного критерия криминализации мошенничества в сфере компьютерной информации выступает объективно существующий пробел в уголовно-правовой охране имущественных отношений. В УК РФ после его принятия долгое время отсутствовала какая-либо норма, предусматривающая уголовную ответственность за хищение чужого имущества с использованием компьютерной информации.[18]

В соответствии со ст. 159.6 УК РФ, мошенничество в сфере компьютерной информации представляет собой хищение чужого имущества или приобре-

[18]Елин В.М. Мошенничество в сфере компьютерной информации как новый состав преступления // Бизнес-информатика. М. 2013. № 2 (24). С. 70-76.

тение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачикомпьютерной информации или информационно-телекоммуникационных сетей.

Согласно пояснительной записке к законопроекту № 53700-6 о дифференциации мошенничества на отдельные составы, российский законодатель, вводя ответственность за мошенничество в сфере компьютерной информации, учитывал, что подобные преступления совершаются не путем обмана или злоупотребления доверием конкретного субъекта, а путем получения доступа к компьютерной системе и совершения вышеуказанных действий, которые в результате приводят к хищению чужого имущества или приобретению права на чужое имущество.

Из диспозиции ст. 159.6 УК РФ следует, что предусмотренное указанной статьей деяние совершается не путем обмана или злоупотребления доверием как все остальные виды мошенничества, а путем использования компьютерной информации. Таким образом, в составе компьютерного мошенничества (ст. 159.6 УК РФ) нет обмана и заблуждения. Их место занимает злоупотребление компьютерной информацией. Это неспециальная норма, а норма, восполняющая пробел.

Российская уголовно-правовая доктрина и российский законодатель исходят из того, что адресатом мошеннического обмана может быть только человек, но не техническое устройство.

Общественную опасность мошенничества в сфере компьютерной информации формируют общественно-опасные последствия в виде имущественного ущерба, причиняемого собственнику или иному владельцу имущества.

Мошенничество в сфере компьютерной информации является общественно-опасным именно в силу того, что соответствующие манипуляции с компьютерной информацией выступают в качестве способа хищения чужого имущества или приобретения права на чужое имущество.

Сами по себе действия с компьютернойинформацией не обязательно свя-

заны с неправомерным доступом к ней. Так пин - код банковской карты может быть доверен виновному самим владельцем карты, например, дляоказания помощи в получении пенсии. Однако, если затем виновный уже без согласия владельца получает другие суммы и обращает в свою пользу, налицо общественно опасное деяние, выражающееся в совершении хищения посредством использования компьютерной информации.[19]

Представляется, что общественную опасность мошенничества в сфере компьютерной информации формирует именно имущественный ущерб, причиняемый потерпевшему. Сами действия с компьютерной информацией рассматриваемые вне связи с хищением чужого имущества или приобретением права на чужое имущество, не обязательно являются общественно-опасными.

Общественную опасность манипуляции с компьютерной информацией приобретают не сами по себе, а в качестве способа совершения хищения, то есть совершенных с корыстной целью противоправных безвозмездного изъятия и/или обращения чужого имущества в пользу виновного или других лиц, причинивших ущерб собственнику или иному владельцу этого имущества (примечание к ст. 158 УК РФ). Здесь можно привести аналогию с «общеуголовным» мошенничеством, предусмотренным в ст. 159 УК РФ, где в качестве способа выступает обман или злоупотребление доверием. Указанные действия сами по себе, вне связи с хищением являются лишь аморальными. Общественную опасность они приобретают, так как выступают в качестве способа хищения чужого имущества или приобретения права на чужое имущество.

Криминализацию «мошенничества в сфере компьютерной информации» (ст. 159.6 УК РФ) следует признать обоснованной, так как она основывается на ясных критериях и позволяет решить ряд проблем, возникающих при квалификации преступлений.

### 2.3 Проблемы квалификации компьютерного мошенничества

Анализируя статью 159.6 УК РФ по прошествии четырех лет с момента

[19] Гарбатович Д.А. Проблемные аспекты эффективности норм, предусматривающих уголовную ответственность за совершение преступлений в сфере компьютерной информации // Библиотека криминалиста. 2013. № 5 (10). С. 40 - 47.

начала ее действия, приходим к выводу о том, что у правоприменителя, как и у представителей научного сообщества, отсутствует единое мнение относительно многих аспектов, присущих рассматриваемому составу и влияющих на квалификацию. В предложенной законодателем редакции данная норма вызвала множество критики, поскольку в ее диспозицию включены крайне спорные признаки, ломающие сложившуюся систему противодействия преступлениям против собственности. Обнаруживаются существенные противоречия применительно к преступлениям всфере компьютерной информации, эти противоречия проявляются как в объекте, так и в квалифицирующих признаках. В настоящее время этот вопрос являетсяактуальным для уголовного законодательства РФ. На законодательном уровнепредложений по поводу решения этой проблемы пока не вносилось, однако, рядучёных высказали свою точку зрения относительно решения этой проблемы.

Одни предлагают ввести в УК РФ специальную статью «Компьютерное мошенничество», под которым понимает завладение чужим имуществом путём обмана, злоупотреблением доверием, присвоения, растратылибо причинение имущественного ущерба путём обмана или злоупотреблениядоверием, совершённое с использованием ЭВМ, системы ЭВМ или их сети.[20]

Однако, другие юристы в опровержение такого предложения говорят о требованиях законодательной техники и отмечают, что каждый применяемый, вданном случае, в уголовном законе, термин должен быть строго определён и иметь одно значение во всех правовых актах. За счёт определённости понятийного аппарата достигается внутренняя согласованность и непротиворечивость уголовного законодательства, повышается эффективность правоприменения, исключаются нарушения закона. То есть, на данном этаперазвития экономического и правового регулирования РФ не сложилось единойточки зрения относительно природы таких преступлений.

Одновременно с этим можно заметить, что по предмету посягательства

[20]Лимонов В.А. Отграничение мошенничества от смежных составов преступления // Законность. 2012. № 3. С. 10-12.

состав мошенничества в сфере компьютерной информации в полной мере соотносится с «материнским» составом.[21]

Объективная сторона мошенничества в сфере компьютерной информации сформулирована своеобразно, в результате формируется мнение о том, что данная форма завладения чужим имуществом с трудом может быть отнесена к группе мошенничества, поскольку характерные для мошенничества признаки – обман или злоупотребление доверием в данной норме не фигурируют.

Ранее Верховный Суд РФ в пояснительной записке разъяснил, что преступления, предусмотренные данной статьей не совершаются классическими для любого мошенничества способами, а именно обманом или злоупотреблением доверием. Субъект лишь получает доступ к соответствующим сведениям, что в результате приводит к хищению чужого имущества или приобретению права на него. В связи с этим, при квалификации данных преступлений возникает проблема необходимости установления факта обмана или злоупотребления доверием.

Так как в диспозиции ст. 159.6 УК РФ заимствуется термин «мошенничество», выступающий в качестве видового для всех специальных составов, предусмотренных ст.ст. 159.1-159.6 УК РФ, это дает полное основание для вывода о необходимости установления факта обмана или злоупотребления доверием и при совершении мошенничества в сфере компьютерной информации, поскольку оно закрепляет специальный состав, основывающийся на «материнском», а следовательно, должен соответствовать ему по общим признакам. С другой стороны, так как законодатель не предусмотрел обман и злоупотребление доверием в качестве признака мошенничества в сфере компьютерной информации, то справедливо было бы именовать данную статью хищением с использованием компьютерной информации, что исключило бы привязку анализируемого состава к мошенничеству.

Возможно, что законодатель, а вслед за ним и правоприменитель допускают обман оборудования, как это, на пример, признается в практике ряда за-

[21] Максимов В.Ю. Компьютерные преступления (вирусный аспект). М.: АО «Центр ЮрИнфор», 2006. С. 210.

рубежных государств, таких как в Великобритании или Германии.

Однако, можно предположить, что лицо, совершающее рассматриваемое преступление, способами, указанными в законе, обманывает, вводит в заблуждение собственника или иное лицо, в результате чего последним причиняется материальный ущерб. Данный вывод подтверждается следующим примером из судебной практики.

Лагузина с целью извлечения материальной выгоды для себя, изготовила в различное время несколько фиктивных трудовых договоров, согласно которым между ЗАО и фиктивно трудоустроенными лицами было достигнуто соглашение об их найме для работы в гипермаркете на должность продавца-кассира. Используя компьютерную программу, виновная вносила в табель учета рабочего времени не соответствующие действительности учетные записи о том, что лица числятся в штате гипермаркета на должности продавца-кассира.

В последующем умышленно не вносила в табели учета рабочего времени отметки о неявке на работу фиктивно трудоустроенных на должность продавца-кассира лиц, посредством сети «Интернет» предоставляла сформированные ею табели учета рабочего времени в бухгалтерию Центрального офиса ЗАО. Заработная плата на фиктивно трудоустроенных перечислялась на расчетные счета, открытые Лагузиной на их имя в одном из отделений Сбербанка РФ.

Примечательно, что если бы фигурантка указанного дела осуществляла преступные операции без использования компьютерных средств, то, очевидно ее деяние квалифицировалось бы по статье 159 УК РФ, и последствия были бы гораздо негативнее.[22]

Способы мошенничества в сфере компьютерной информации заключаются в совершении таких операций, как:

- ввод компьютерной информации;
- удаление компьютерной информации;
- блокирование компьютерной информации;

[22]Обзор судебной практики Верховного суда РФ по уголовным делам от 23 декабря 2015 г. № 4 // Бюллетень Верховного Суда РФ. 2016. № 9. С. 53 – 65.

- модификация компьютерной информации;

- иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

При совершении рассматриваемого преступления виновное лицо может совершить одно действие, образующее объективную сторону, либо выполнить несколько указанных действий.

Многие признаки, отраженные в ст. 159.6 УК РФ, ранее были закреплены в ст. 272 УК РФ (Неправомерный доступ к компьютерной информации) и ст. 273 УК РФ (Создание, использование и распространение вредоносных компьютерных программ), что требует обязательного сравнения данных составов. В частности, в примечании к ст. 272 УК РФ закреплена важнейшая дефиниция «компьютерная информация», под которой понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. В отношении данной дефиниции учеными высказывается справедливая критика. Так, некоторые замечают, что используемая в примечании к ст. 272 УК РФ формулировка, распространяющаяся и на ст. 159.6 УК РФ, себя изжила в силу внедрения и использования новых технологий, которые не включаются в модель сформулированного определения.

Использование в диспозиции обобщающего термина «иное вмешательство в функционирование средства хранения, обработки или передачи компьютерной информации» позволяет сделать вывод о том, что способы совершения преступления могут быть различными. Данная формулировка неконкретна, что может породить возможность чрезмерно широкого и неправильного применения термина[23].

Необходимо так же обратить внимание на то, что использованное понятие удаления информации дает возможность избежать квалификации состава

[23]Завидов Б.Д. Обычное мошенничество и мошенничество в сфере высоких технологий // Юрист. 2002. № 7. С. 48 – 54.

преступления, так как затирание компьютерной информации по сути не является удалением. Возможно, более уместным было бы заимствование термина «уничтожение», упоминающегося в ст. 272 УК РФ.

Однако перечень способов вмешательства не является исчерпывающим, что дает возможность использовать любой (нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации, нарушение правил доступа к сетям и прочее).

Под средствами хранения, обработки или передачи компьютерной информации понимаются жесткие диски, оптические диски, USB–накопители, карты памяти, серверное оборудование, рабочие станции, каналы связи.

Преступление, предусмотренное ст. 159.6 УК РФ может быть совершено путем только активных действий. Виновный может осуществить удаленный доступ, либо непосредственно воздействовать на средства хранения, обработки или передачи данных, которые используются при совершении финансовых и других операций в различных организациях.

При сравнении мошенничества в сфере компьютерной информации со смежными составами преступлений, в частности со ст. 272 УК РФ, обращает на себя внимание несогласованность при установлении крупного размера и крупного ущерба. Статья 159.6 УК РФ определяет крупный размер в сумме свыше 1,5 млн. рублей, а статья 272 УК РФ – свыше 1 млн. рублей.

В пункте 12 постановления № 51 Верховного Суда, которое на сегодняшний день утратило свою актуальность, отмечается, что при совершении мошеннических действий с неправомерным внедрением в чужую информационную систему или с иным неправомерным доступом к охраняемой законом компьютерной информации кредитных учреждений либо с созданием заведомо вредоносных программ для ЭВМ, внесением изменений в существующие программы, использованием или распространением вредоносных программ для ЭВМ такие действия квалифицировались по совокупности преступлений как мошенничество (ст. 159 УК РФ) и соответствующее преступление в сфере компьютерной информации (гл. 28 УК РФ).

В настоящее время, в связи с вступлением в силу Федерального Закона № 207 такая квалификация преступлений по совокупности более не потребуется.

Это обстоятельство приводит к выводу о явном несоответствии санкции ст. 159.6 УК РФ характеру и степени общественной опасности описываемого ею деяния. Например, если раньше при квалификации мошенничества в системе интернет-банкинга по совокупности ч. 4 ст. 159 и ч. 1 ст. 272 УК РФ максимальный срок наказания в виде лишения свободы составлял 12 лет, то теперь при квалификации данного преступления по ч. 4 ст. 159.6 УК РФ данный срок ограничен 10 годами.[24]

Кроме того, действующая редакция ст. 15 УК РФ позволяет суду при определенных условиях снизить категорию совершенного преступления на одну степень, то есть признать мошенничество в сфере компьютерной информации, совершенное при наличии признаков части 4 (организованной группой либо в особо крупном размере) преступлением средней тяжести. Это может предоставить виновному новые привилегии в виде возможности освобождения от уголовной ответственности в связи с деятельным раскаянием (ст. 75 УК РФ) или в связи с примирением с потерпевшим (ст. 76 УК РФ), что еще более дискредитирует предупредительную функцию уголовного законодательства.

В любом случае, в первую очередь законодателю, необходимо выработать эффективный способрешения этой проблемы, так как граждане под влиянием различных факторов(политических, экономических, социальных) зачастую идут на совершение такихпреступлений.

Таким образом, можно сделать выводы, что мошенничество в сфере компьютерной информации является закономерным шагом интеграции российского законодательства о борьбе с компьютерными преступлениями в международное.

Статья 159.6 УК РФ состоит из четырех частей, первая из которых рас-

[24]Уголовный кодекс Российской Федерации от 13 июня 1996 г. №63-ФЗ (в ред. от 07 февраля 2017 г.) // Собрание законодательства РФ. 1996. № 25. С. 4153 – 4527.

крывает понятие мошенничества в сфере компьютерной информации, 2, 3 и 4 части указанной статьи содержат квалифицированные составы данного преступления по признакам:

- деяния, совершенного группой лиц по предварительному сговору (ч. 2);

- с причинением значительного ущерба гражданину (ч. 2);

- совершения лицом с использованием своего служебного положения (ч. 3);

- совершения в крупном размере (ч. 3);

- совершения организованной группой (ч. 4);

- совершения в особо крупном размере (ч. 4).

Преступление, предусмотренное ч. 1 ст. 159.6 УК РФ является преступлением небольшой степени тяжести, преступления, предусмотренные ч. 2 и 3 ст. 159.6 УК РФ – преступлениями средней тяжести, а преступления, предусмотренные ч. 4 указанной статьи, – отнесены к тяжким.

Анализ указанной статьи позволяет сделать следующие выводы:

1. Включение мошенничества в сфере компьютерной информации в состав гл. 21 УК РФ предусматривает в качестве видового объекта отношения собственности, непосредственным объектом выступает чужое имущество или права на него.

2. Объективную сторону мошенничества в сфере компьютерной информации составляет хищение чужого имущества или приобретение права на чужое имущество.

3. Способом совершения преступления выступает: ввод, удаление, блокирование, модификация компьютерной информации; иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно - телекоммуникационных сетей.

4. Субъект – общий, по ч. 3 ст. 159.6 УК РФ – специальный, квалифицирующими признаками выступает совершение преступления группой лиц по предварительному сговору, либо организованной группой.

5. Субъективная сторона предполагает прямой умысел. Виновный осознает, что завладевает чужим имуществом или правами на него путем ввода, удаления, блокирования, модификации компьютерной информации либо иным вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

В качестве главного критерия криминализации мошенничества в сфере компьютерной информации выступает объективно существующий пробел в уголовно-правовой охране имущественных отношений.

Из диспозиции ст. 159.6 УК РФ следует, что предусмотренное указанной статьей деяние совершается не путем обмана или злоупотребления доверием как все остальные виды мошенничества, а путем использования компьютерной информации. Таким образом, в составе компьютерного мошенничества (ст. 159.6 УК РФ) нет обмана и заблуждения. Их место занимает злоупотребление компьютерной информацией. Это не специальная норма, а норма, восполняющая пробел.

Общественную опасность мошенничества в сфере компьютерной информации формируют общественно-опасные последствия в виде имущественного ущерба, причиняемого собственнику или иному владельцу имущества.

Мошенничество в сфере компьютерной информации является общественно-опасным именно в силу того, что соответствующие манипуляции с компьютерной информацией выступают в качестве способа хищения чужого имущества или приобретения права на чужое имущество.[25]

Криминализацию «мошенничества в сфере компьютерной информации» (ст. 159.6 УК РФ) следует признать обоснованной, так как она основывается на ясных критериях и способствует конкретизации компьютерных преступлений, наряду с преступлениями в сфере компьютерной информации выделяя преступления, осуществляемые с использованием компьютерных средств. Однако

[25]Елин В.М. Мошенничество в сфере компьютерной информации как новый состав преступления // Бизнес-информатика. 2013. № 2 (24). С. 70-76.

включение данного состава преступления в уголовное законодательство Российской Федерации порождает также ряд проблем, возникающих при квалификации преступлений.

В предложенной законодателем редакции данная норма вызвала множество критики, поскольку в ее диспозицию включены крайне спорные признаки. Обнаруживаются существенные противоречия применительно к преступлениям в сфере компьютерной информации, эти противоречия проявляются как в объекте, так и в квалифицирующих признаках.

Так законодатель не предусмотрел обман и злоупотребление доверием в качестве признака мошенничества в сфере компьютерной информации, то справедливо было бы именовать данную статью хищением с использованием компьютерной информации, что исключило бы привязку анализируемого состава к мошенничеству.

Способы мошенничества в сфере компьютерной информации заключаются в совершении таких операций, как:

- ввод компьютерной информации;
- удаление компьютерной информации;
- блокирование компьютерной информации;
- модификация компьютерной информации;
- иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

При совершении рассматриваемого преступления виновное лицо может совершить одно действие, образующее объективную сторону, либо выполнить несколько указанных действий.

Однако перечень способов вмешательства не является исчерпывающим, что дает возможность использовать любой (нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации, нарушение правил доступа к сетям и прочее).

Преступление, предусмотренное ст. 159.6 УК РФ может быть совершено

путем только активных действий.

Таким образом, термин «компьютерное мошенничество» не отвечает характеристике мошенничества. Любые виды хищения с применением компьютерных технологий необходимо вводить в качестве квалифицирующего признака кражи (ст. 158 УК РФ), когда речь идет не об обмане конкретных потерпевших с использованием ИТ технологий, а именно как это предусмотрено нормами ст. 159.6 УК РФ, «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»  или же вводить дополнительные статьи, регулирующих ответственность за любые виды хищения с применением компьютерных технологий.

Кроме того действующее уголовное законодательство остро нуждается в закреплении в нем норм, которые в качестве конструктивного признака включают способ, связанный с преступным использованием компьютерной информации. В качестве квалифицирующего признака отдельных составов преступлений необходимо предусмотреть совершение преступного деяния с использованием информационно-телекоммуникационных или компьютерных систем. Данная необходимость обусловлена реалиями современной жизни и повсеместным использованием, в том числе для совершения противоправной деятельности высокотехнологичных устройств. В то же время существующий уголовно-правовой механизм, который должен обеспечивать эффективное предупреждение распространения подобных общественно опасных проявлений, должным образом не сформировался.

Также, необходимо отметить, что на территории Российской Федерации борьбу с мошенничеством реализуют в основном органы МВД, отделов по борьбе с экономическими преступлениями УВД. В некоторых ГУВД существуют специализированные отделы по борьбе с мошенничеством, однако, отделов по борьбе с «кибермошенничеством» не предусмотрено, поэтому в целях

эффективной работы в данной сфере, наличия необходимого уровня безопасности общества от «кибермошенничества», безусловно, необходимо создание компетентных органов и структурных подразделений, имеющих квалифицированных специалистов. Так же действующее уголовное законодательство остро нуждается в закреплении в нем норм, которые в качестве конструктивного признака включают способ, связанный с преступным использованием компьютерной информации.

# 3 ПРОБЛЕМЫ ПРАВОПРИМЕНИТЕЛЬНОЙ ПРАКТИКИ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

## 3.1 Анализ судебной практики по делам о мошенничестве в с компьютерной информации

Федеральным законом от 29 ноября 2012 г. № 207-ФЗ Уголовный кодекс дополнен нормой об ответственности за мошенничество в сфере компьютерной информации. В пояснительной записке к проекту авторы законопроекта так обосновали предложения о дополнении уголовного закона указанной нормой: «Предлагается также выделить в самостоятельный состав преступления мошенничество в сфере компьютерной информации (ст. 159.6 законопроекта), когда хищение или приобретение права на чужое имущество сопряжено с преодолением компьютерной защиты имущества (имущественных прав) и осуществляется путем ввода, удаления, модификации или блокирования компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Подобные преступления совершаются не путем обмана или злоупотребления доверием конкретного субъекта, а путем получения доступа к компьютерной системе и совершения вышеуказанных действий, которые в результате приводят к хищению чужого имущества или приобретению права на чужое имущество».[26]

Способом совершения преступления в ст. 159.6 УК РФ названы такие действия, как ввод, удаление, блокирование, модификация, иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Таким образом, обман и злоупотребление доверием способами совершения компьютерного мошенничества не являются. Следовательно, законодатель предусмотрел ответственность за новую форму хищения.

[26]Южин А.А. Дискуссионные вопросы мошенничества в сфере компьютерной информации // Право и кибербезопасность. 2014. № 2. С. 35 - 39.

Проведенные исследователями обобщения судебной практики показывают, что по ст. 159.6 УК квалифицируются действия, состоящие, в частности, в использовании:

- подложного (от имени владельца счета) электронного платежного поручения, направляемого через систему «Банк-Клиент», что предполагает незаконное, помимо воли клиента и банка, проникновение в компьютерную систему, ввод и модификацию информации и влечет перечисление средств на счет, которым может пользоваться виновный;

- программы, предназначенной для несанкционированной модификации компьютерной информации, когда такая программа устанавливается на компьютер собственника имущества (например, в бухгалтерии организации). С помощью программы дистанционного банковского обслуживания расчетного счета виновные направляют подложное платежное поручение о перечислении средств на контролируемые ими счета;

- программы для удаления файла платежного поручения, направленного владельцем счета в банк посредством электронной системы «Банк-Клиент», и замены этого файла на подложный, содержащий реквизиты счета, подконтрольного виновному лицу;

- банковской карты организации, когда виновный осуществляет вмешательство в функционирование компьютера организации, получив удаленный несанкционированный доступ к управлению ее расчетным счетом и затем похищая с данного счета денежные средства (за исключением случая хищения их в наличной форме);

- ошибочно подключенной к номеру телефона услуги мобильного банка, предоставляющей право распоряжаться денежными средствами, находящимися на счете другого лица (бывшего владельца телефонного номера);

- полученных путем неправомерного доступа (путем использования специальных программ и системы удаленного доступа в сети Интернет) логинов и паролей, посредством которых владелец счета управляет движением денежных средств на своем счете, для направления в банк (также через сеть Интернет)

распоряжения о перечислении средств на подконтрольные виновному счета (при этом используются компьютерные системы - посредники, позволяющие скрыть реальный IP-адрес компьютера в сети Интернет);

- незаконно полученных по поддельной доверенности дубликата сим-карты гражданина и информации о его банковских счетах для несанкционированного входа в компьютерную программу удаленного доступа к счетам клиентов «Банк - Онлайн» через сеть Интернет и направления распоряжения о перечислении средств на подконтрольный виновному счет и другие.[27]

Проанализируем некоторые примеры способов мошенничества в сфере компьютерной информации из судебной практики.

Гражданин Н., находясь в торгово-развлекательном центре, реализуя свой преступный умысел, направленный на хищение денежных средств, обратился с просьбой к гражданину С. воспользоваться его банковской картой с целью установления интернет-обслуживания. При этом Н. дезинформировал С., который, не подозревая о преступных намерениях Н., осуществил в банкомате с использованием своей карты операции, продиктованные Н., и предоставил ему две выданные банкоматом квитанции с данными о своей банковской карте и о находящихся на ней денежных средствах. Завладев конфиденциальной информацией, Н. перевел денежные средства в размере 12000 рублей с банковской карты С. на банковскую карту своего знакомого З. через Интернет. Далее Н., используя банковскую карту З., получил похищенные денежные средства в банкомате. В результате тайного хищения потерпевшему С. причинен значительный ущерб.

Президиум Алтайского краевого суда переквалифицировал действия Н. с п. «в» ч. 2 ст. 158 УК РФ на ч. 2 ст. 159.6 УК РФ, в обоснование своего решения указав следующее: «Судом действия Н. квалифицированы по ч. 2 ст. 159 УК РФ как хищение чужого имущества, совершенное путем обмана, с причинением значительного ущерба потерпевшему. Решение кассационной инстанции о пе-

[27]Обзор судебной практики Верховного суда РФ по уголовным делам от 23 декабря 2015 г. № 4 // Бюллетень Верховного Суда РФ. 2016. № 9. С. 57 – 78.

реквалификации действий Н. с ч. 2 ст. 159 УК РФ на ч. 2 ст. 158 УК РФ следует признать ошибочным. Судебная коллегия мотивировала свои выводы тем, что действие осужденного по изъятию денежных средств является тайным, а обман потерпевшего явился средством облегчения совершения хищения. При этом коллегией не учтен особый способ совершения хищения, выделенный законодателем в отдельный состав преступления и являющийся специальной нормой по отношению к ст. 159 УК РФ.

Как установлено судом, осужденный путем обмана завладел информацией о реквизитах банковской карты потерпевшего, после чего получил возможность посредством электронной системы через Интернет управлять счетом гражданина С. и перевел с его банковской карты денежные средства на другой счет. Таким образом, описанный способ хищения свидетельствует о вмешательстве в функционирование средств хранения, обработки, передачи компьютерной информации, что подпадает под действие ст. 159.6 УК РФ».[28]

Приведенный пример показывает, что обман как способ совершения хищения не характерен для компьютерного мошенничества. Обман выступил не способом изъятия и обращения чужого имущества в пользу виновного, а способом завладения конфиденциальной информацией, которая в последующем выступила средством совершения компьютерного мошенничества. В данном случае обман находился за рамками объективной стороны компьютерного мошенничества, он относится к подготовительной стадии хищения, а потому на квалификацию деяния не влияет. Само же хищение обоснованно признано оконченным не в момент получения виновным в банкомате наличных денег со счета гражданина З., а с момента зачисления их на указанный счет, когда денежные средства еще не обрели вещественную форму и потому не могли согласно доктрине и сложившейся судебной практике рассматриваться как предмет кражи.

Другой пример: гражданин О., обвинялся в том, что в период с декабря 2011 г. по ноябрь 2012 г., используя приложение ICQ (централизованная служ-

[28]Постановление Президиума Алтайского краевого суда от 03 сентября 2013 г. по делу № 44у224/13 [Электронный ресурс]. URL http://www.consultant.ru. (дата обращения: 15.10.2016).

ба для мгновенного обмена сообщениями в сети Интернет), установленное на своем мобильном телефоне («Нокиа - Е52»), знакомился и устанавливал доверительные отношения с пользователями ICQ с целью совершения мошенничества - хищения чужого имущества путем обмана. В дальнейшем О., под различными предлогами получал от пользователей ICQ доступ к их учетным записям в данном мобильном приложении, после чего рассылал от имени этих лиц другим пользователям ICQ сообщения в виде просьб о перечислении денежных средств на телефонные номера оператора сотовой связи «Билайн». После поступления денежных средств на подконтрольные гражданину О., абонентские номера он распоряжался ими по своему усмотрению. Действия обвиняемого О., квалифицированы судом как мошенничество в сфере компьютерной информации с причинением значительного ущерба гражданину, совершенное путем обмана и злоупотребления доверием, то есть, как преступление, предусмотренное ч. 2 ст. 159.6 УК РФ.[29]

В данном случае, уголовный закон применен неверно. Деяние, совершенное гражданином О., подпадает под признаки состава преступления, предусмотренного ч. 2 ст. 159 УК РФ, поскольку способом совершения преступления выступил мошеннический обман. Именно обман, который по форме являлся электронным текстовым сообщением, а по содержанию представлял собой искаженные сведения, воспринимаемые потерпевшими как истинные, и послужил способом введения их в заблуждение, и как результат такого заблуждения повлек передачу имущества виновному.

В отличие от первого примера в данном деле обман являлся обязательным признаком объективной стороны мошенничества. Даже если считать, что ввод компьютерной информации и иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации со стороны подсудимого О., имели место, то они относились не к объективной стороне завладения чужим имуществом, ак его подготовительной стадии.

[29]Приговор суда республики Дагестан по делу № 1-28/2013 // Дагестанские Огни Республики: [Электронный ресурс]. URL: http://www.gcourts.ru/case/22900134 (дата обращения: 10.09.2016).

Как покушение на совершение компьютерного мошенничества следует оценивать и случаи, когда лицо не имело возможности распорядиться похищенным имуществом вследствие того, что, например, расчетный счет в банке, на котором аккумулировались денежные средства, изначально был заблокирован кредитной организацией.

Дискуссионным так же является вопрос о квалификации содеянного, как покушение в ситуациях группового компьютерного мошенничества, когда момент «приобретения лицом реальной возможности распорядиться похищенным» обусловлен совершением действий третьими лицами.

С одной стороны, представляется логичным, что такое хищение следует считать оконченным с того момента, когда возможность по распоряжению имуществом возникла хотя бы у одного из лиц, входящих в группу. Соответственно, если согласно распределению ролей похищенное имущество накапливается на банковском счете одного из злоумышленников, то поступление средств на этот счет уже само по себе свидетельствует об оконченном составе преступления в действиях всех соучастников. И наоборот: отсутствие такой возможности у конкретного лица позволяет сделать вывод о покушении на мошенничество в сфере компьютерной информации.

В судебной практике не всегда эти обстоятельства учитываются надлежащим образом. Так, граждане Ф., Б., и Д. признаны виновными в совершении мошенничества в сфере компьютерной информации группой лиц по предварительному сговору в крупном размере.

В порядке обжалования вынесенного приговора сторона защиты указывала на несостоятельность квалификации действий осужденных по ч. 3 ст. 159.6 УК РФ как оконченный состав преступления, поскольку Ф., Б., и Д. не могли распорядиться по своему усмотрению денежными средствами, так как деньги находились на счете в банке и не могли быть перечислены куда-либо в связи с тем, что номинальный директор организации и уполномоченный распорядитель счета гражданка П. была задержана правоохранительными органами непосредственно в банке. По небезосновательному мнению защиты, в такой ситуации

имело место покушение, и действия надлежало квалифицировать по ч. 3 ст. 30 и ч. 3 ст. 159.6 УК РФ.

Как представляется, вывод суда, что преступления, совершенные Ф., Б., и Д., во всех трех эпизодах носят оконченный характер, является спорным. В данном примере появление у виновных реальной возможности распорядиться похищенными денежными средствами напрямую зависело от ее возникновения у третьего лица - номинального руководителя организации. А потому в случае его заблаговременного задержания содеянное всех соучастников необходимо было квалифицировать как покушение на совершение мошенничества в сфере компьютерной информации.[30]

Таким образом позиция, сформулированная в Постановлении Пленума Верховного Суда РФ от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате», согласно которой с момента зачисления денег на банковский счет лица оно получает реальную возможность распоряжаться поступившими денежными средствами по своему усмотрению, может иметь вполне конкретные исключения. Иными словами, представляется возможной ситуация, когда деньги на счет виновного могут поступить, но реальная возможность по их распоряжению не возникнет (например, в случае блокировки счета по совершению расходных операций).

Согласно приговору гражданин Г., имея умысел на тайное хищение чужого имущества, а именно денежных средств ОАО АКБ «ХХХ» в крупном размере, приискал для совершения преступления необходимые комплектующие и материалы, из которых изготовил два приспособления. Первое устройство позволяло получать (перехватывать) информацию, вводимую держателями карт посредством клавиатуры банкомата, а именно ПИН-коды банковских карт, а второе обеспечивало получение (перехват) информации с магнитных полос банковских пластиковых карт.

Для реализации своих преступных намерений Г., прибыл в дополнитель-

[30]Приговор Московского городского суда от 24 апреля 2013 г. по делу № 10-2268/2013 года [Электронный ресурс]. Доступ из справочно-правовой системы «Гарант».

ный офис ОАО АКБ «ХХХ», где под видом монтажа устройства, контролирующего доступ в помещение с банкоматом, установил на входную дверь изготовленное им приспособление для получения (перехвата) информации с магнитных полос банковских пластиковых карт. Таким образом, Г., умышленно создал условия, при которых доступ к банкомату дополнительного офиса ОАО АКБ «ХХХ» стал возможен лишь после копирования компьютерной информации с магнитной полосы банковской пластиковой карты в память указанного устройства. Второе изготовленное им приспособление Г., установил непосредственно над экраном лицевой панели банкомата для получения (перехвата) информации, вводимой клиентами банка с клавиатуры банкомата, а именно ПИН-кодов банковских карт, после чего с места преступления скрылся.

Для прохода к банкомату в вышеуказанном офисе клиенты ОАО АКБ «ХХХ» сканировали свои банковские карты через установленное на входной двери гражданином Г. приспособление, в результате чего записанная на магнитной полосе пластиковых карт компьютерная информация копировалась в память устройства. Остаток денежных средств на счетах, к которым были прикреплены сканированные карты, варьировался от нескольких рублей до нескольких сотен тысяч рублей и составил в общей сумме 487521 рубль 10 копеек.

При попытке демонтировать установленные им устройства для того, чтобы использовать скопированную и сохраненную в их памяти компьютерную информацию с магнитных полос банковских карт и ПИН-коды к ним с целью тайного хищения в крупном размере находящихся на счетах денежных средств, принадлежащих ОАО АКБ «ХХХ», гражданин Г. был задержан и потому довести свой преступный умысел до конца не смог по независящим от него обстоятельствам. Г. осужден за приготовление к краже в крупном размере, а также за неправомерный доступ к охраняемой законом компьютерной информации, повлекший копирование компьютерной информации, совершенный из корыстной заинтересованности (ч. 1 ст. 30 УК РФ, п. «в» ч. 3 ст. 158 УК РФ, ч. 2 ст. 272 УК РФ).

Обоснованность подобной квалификации вызывает сомнения в части квалификации по ст. 158 УК РФ. Попутно отметим, что деяние, предусмотренное ч. 2 ст. 272 УК РФ (по признаку «совершенное из корыстной заинтересованности») оценено судом верно как оконченное преступление вне зависимости от того, появилась ли у субъекта преступления реальная возможность воспользоваться неправомерно скопированной компьютерной информацией, преступление окончено согласно конструкции состава в момент наступления одного или нескольких из указанных в законе последствий, в нашем случае имело место копирование информации.[31]

Что же касается посягательства на собственность, то в данном случае имел место прямой не конкретизированный (неопределенный) умысел. Виновный, стремясь похитить как можно больше денежных средств, не мог наверняка знать, каким будет преступный результат: скольким потерпевшим и в какой сумме им будет причинен ущерб. Исходя из теории квалификации, при наличии не конкретизированного прямого умысла содеянное квалифицируется по фактически наступившим последствиям. Если при не конкретизированном умысле последствия не наступили по причинам, не зависящим от воли виновного, то его общественно опасное поведение следует квалифицировать как приготовление (покушение) на причинение наименее опасного из всех желаемых вредных последствий. Такое правило квалификации при не конкретизированном умысле вытекает из принципа необходимости толкования любого сомнения в пользу обвиняемого.

Если бы субъект преступления довел свой умысел до конца, то потерпевшим стала бы кредитная организация при условии, что физические лица, со счетов которых были бы похищены денежные средства, успели бы воспользоваться правом, закрепленным в п. п. 11 и 12 ст. 9 Федерального закона от 27 июня 2011 г. № 161 «О национальной платежной системе». Но предположим, что кто-то из держателей пластиковых карт не успел своевременно оповестить

[31] Апелляционное определение Московского городского суда от 04 сентября 2013 г. по делу № 10-6391 [Электронный ресурс]. URL: http://www. justicemaker.ru/primers.php (дата обращения: 01.11.2016).

кредитную организацию о неправомерном списании денежных средств, в таком случае потерпевшими будут и ООО АКБ «ХХХ», и указанное физическое лицо, которому банк, стало быть, не возместит утраченные средства. Как видно, квалификация будет зависеть от конкретных обстоятельств дела и фактически наступивших последствий.

Здесь указывается, что «в случае утраты электронного средства платежа и (или) его использования без согласия клиента клиент обязан направить соответствующее уведомление оператору по переводу денежных средств в предусмотренной договором форме незамедлительно после обнаружения факта утраты электронного средства платежа и (или) его использования без согласия клиента, но не позднее дня, следующего за днем получения от оператора по переводу денежных средств уведомления о совершенной операции" (п. 11), тогда как "после получения оператором по переводу денежных средств уведомления клиента в соответствии с ч. 11 настоящей статьи оператор по переводу денежных средств обязан возместить клиенту сумму операции, совершенной без согласия клиента после получения указанного уведомления» (п. 12).

Допустим, что в рассматриваемом нами случае виновному удалось достичь преступного результата он сумел получить доступ к неправомерно скопированной компьютерной информации, а затем, используя специальное техническое устройство «инкодер», подключенное к персональному компьютеру, а также соответствующее программное обеспечение, изготовил дубликаты банковских карт их владельцев и, имея ПИН-коды, получил в банкомате денежные средства. В этом случае охраняемая законом компьютерная информация, скопированная с магнитных полос банковских карт, выступила бы средством совершения преступления, а ввод ПИН-кода с клавиатуры банкомата выступил бы способом хищения.

В этом случае число самостоятельно квалифицируемых преступных эпизодов зависело бы от числа потерпевших. Если потерпевшим оказывается только банк, то все операции по введению информации имели бы результатом причинение ущерба лишь одному потерпевшему банку. Стало быть, содеянное об-

разовывало бы единое продолжаемое преступление, совокупности здесь не будет. В этом случае содеянное квалифицировалось бы по ч. 1 ст. 159.6 УК РФ, так как крупный размер хищения должен превышать один миллион пятьсот тысяч рублей. Однако если потерпевшими в силу приведенных выше причин окажутся и банк, и физические лица, то содеянное надлежит квалифицировать по совокупности преступлений, предусмотренных ст. 159.6 УК РФ. Поскольку же криминальная деятельность лица была пресечена на подготовительном этапе, то его ответственность по ч. 1 ст. 30 и ч. 1 ст. 159.6 УК РФ исключается (с учетом, как обосновано нами выше, правил квалификации при неконкретизированном умысле) в силу ч. 2 ст. 30 УК РФ.

Согласно абз. 2 п. 16 Постановления Пленума Верховного Суда РФ от 27 декабря 2002 г. № 29 «О судебной практике по делам о краже, грабеже и разбое» «От совокупности преступлений следует отличать продолжаемое хищение, состоящее из ряда тождественных преступных действий, совершаемых путем изъятия чужого имущества из одного и того же источника, объединенных единым умыслом и составляющих в своей совокупности единое преступление».

ПИН - код был получен не посредством неправомерного доступа к компьютерной информации, а с помощью камеры, установленной над экраном лицевой панели банкомата. Следовательно, эти действия находились за рамками объективной стороны состава мошенничества в сфере компьютерной информации, предшествовали ей и требуют дополнительной квалификации.

Но даже если предположить, что неправомерный доступ к компьютерной информации охватывается таким признаком преступления, предусмотренного ст. 159.6 УК РФ, как иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации, и является способом совершения данного преступления (мошенничества в сфере компьютерной информации), такой доступ, при условии, что он повлек указанные в ст. 272 УК РФ последствия, нуждается в самостоятельной уголовно-правовой оценке, поскольку данное деяние (хищение из банкомата) посягает на два различных объекта уголовно-правовой охраны.

Таким образом, можно сделать вывод, что обман, как способ совершения хищения не характерен для компьютерного мошенничества. Обман выступает способом завладения конфиденциальной информацией, которая в последующем выступает средством совершения компьютерного мошенничества.

Кроме того, хищение денежных средств путем перевода со счета потерпевшего на счет преступника обоснованно признано оконченным с момента зачисления их на указанный счет. Однако встречаются случаи, когда лицо не имело возможности распорядиться похищенным имуществом вследствие того, что, например, расчетный счет в банке, на котором аккумулировались денежные средства, изначально был заблокирован кредитной организацией. Такие ситуации следует оценивать  как покушение на совершение мошенничества в сфере компьютерной информации.

Что касается группового компьютерного мошенничества, то хищение следует считать оконченным с того момента, когда возможность по распоряжению имуществом возникла хотя бы у одного из лиц, входящих в группу. То есть, если согласно распределению ролей похищенное имущество накапливается на банковском счете одного из злоумышленников, то поступление средств на этот счет уже само по себе свидетельствует об оконченном составе преступления в действиях всех соучастников. И наоборот: отсутствие такой возможности у конкретного лица позволяет сделать вывод о покушении на мошенничество в сфере компьютерной информации.

Так как обман являлся обязательным признаком объективной стороны мошенничества, то, если считать, что ввод компьютерной информации и иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации со стороны подсудимого имеют место быть, то они относятся не к объективной стороне завладения чужим имуществом, а к его подготовительной стадии.

Так же, исходя из теории квалификации, при наличии не конкретизированного прямого умысла содеянное квалифицируется по фактически наступившим последствиям. И если при не конкретизированном умысле последствия не

наступили по причинам, не зависящим от воли виновного, то его общественно опасное поведение следует квалифицировать как приготовление (покушение) на причинение наименее опасного из всех желаемых вредных последствий. То есть, любые сомнения толкуются в пользу обвиняемого.

Если, неправомерный доступ к компьютерной информации охватывается таким признаком преступления, как иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации, и является способом совершения мошенничества в сфере компьютерной информации, такой доступ, при условии, что он повлек указанные в ст. 272 УК РФ последствия, нуждается в самостоятельной уголовно-правовой оценке, поскольку данное деяние как на пример, хищение денежных средств из банкомата, посягает на два различных объекта уголовно-правовой охраны.

В общем,сравнение санкций ст. 272 УК РФ и ст. 159.6 УК РФ показывает, что неправомерный доступ является более общественно опасным преступлением. Следовательно, хищение из банкомата нуждается в дополнительной квалификации со ст. 272 УК РФ. Подавляющее большинство криминалистов сходятся во мнении, что объективная сторона мошенничества в сфере компьютерной информации не охватывает собою действия (бездействие), закрепленные в гл. 28 УК РФ.

Судами мошенничество в сфере компьютерной информации рассматривается как новая форма хищения, как это и предусмотрено законодательством, и большинство криминалистов разделяют данный подход. И потому, Верховному Суду в Постановлении Пленума от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» необходимо пересмотреть позицию в части квалификации хищения из банкомата посредством поддельной платежной карты, признав, что в данном случае совершается не кража, а мошенничество в сфере компьютерной информации.

### 3.2 Актуальные проблемы расследования мошенничества в сфере компьютерной информации

В условиях совершенствования глобальных информационно-

телекоммуникационных технологий, формирования единого мирового информационного пространства, а также вследствие отсутствия единообразного законодательного регулирования общественных отношений, связанных с использованием информационных ресурсов сети Интернет, как на национальном, так и на международном уровне отечественные правоохранительные органы оказались не в полной мере готовы эффективно противостоять новым видам преступных посягательств – киберпреступлениям, среди которых, одним из самых распространенных является мошенничество в сфере компьютерной информации.

Проблема борьбы с данным видом мошенничества в последнее время становится одной из серьезных угроз для личности и государства и поэтому является одной из приоритетных задач правоохранительных органов России.

Норма мошенничество в сфере компьютерной информации была введена в УК РФ в 2012 году и по данным МВД Амурской области с 2012 года по октябрь 2016 года количество таких преступлений увеличивается.[32] Так в 2012 году правоохранительными органами не было зарегистрировано ни одного преступления, в 2013 году их количество было так же равно нулю, а вот в 2014 году их количество составило 2, в 2015 году так же 2 преступления о мошенничестве в сфере компьютерной информации в 2016 году эта цифра достигла показателя 3 преступлений.

Таким образом, согласно данным статистики мошенничество в сфере компьютерной информации становится все более распространенным преступлением. Однако, так как данная норма, была введена в УК РФ сравнительно недавно, то существует ряд проблем, с которыми сталкиваются следователи и дознаватели в процессе расследования данных преступлений.

В рамках дипломной работы было проведено анкетирование, среди сотрудников следственных отделов и отделов дознания Амурской области. Всего было опрошено 70 сотрудников различных отделов. В ходе данного исследова-

[32] Статистическая база данных ИЦ ГУ МВД России по Амурской области [Электронный ресурс]. Доступ из справочно-правовой системы «КонсультантПлюс».

ния были сделаны следующие выводы.

Одной из проблем расследования мошенничества в сфере компьютерной информации является недостаточная компетентность лиц, которые занимаются их выявлением и раскрытием.

Так, например, 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 все 95 % опрошенных следователей назвали источником знаний компьютерных технологий самообразование, и только 5 % - специальное образование.

Большинство следователей (дознавателей) отметили, что имеющихся знаний для расследования компьютерного мошенничества недостаточно. Для решения данной проблемы, по мнению опрошенных, необходимо проведение их обучения по расследованию данного вида преступлений, а также организация семинаров, посвященных модификации компьютерных технологий.

Другой проблемой является несвоевременность выявления компьютерного. Как показали результаты проведенных исследований, в 53 % случаев с момента совершения преступления до поступления информации о совершенном преступлении проходит более 5 дней.

Несвоевременность выявления преступлений отметили 75 % опрошенных следователей. Очевидно, что запоздалое начало предварительного расследования может привести к безвозвратной утрате важных доказательств, увеличению сроков предварительного расследования и другим негативным последствиям. Как правило, несвоевременное выявление таких преступлений влечет за собой опасность уничтожения следов их совершения.

При расследовании мошенничества в сфере компьютерной информации

чаще всего проводятся такие следственные действия, как осмотр места происшествия (указали 79 % опрошенных), допрос (68 %), обыск (63 %), выемка (37 %) и назначение судебных экспертиз (47 %). Наибольшие трудности возникают при проведении осмотра места происшествия (это отметили 42 % опрошенных) и назначении судебных экспертиз (37 % опрошенных).

Примечательно, что 21 % из числа опрошенных практических работников не проводили осмотр места происшествия и отметили, что причиной отказа от проведения осмотра места происшествия является отсутствие места происшествия. Это значит, что распознавание места совершения таких преступлений невозможно без установления обстановки совершения преступления, которая чаще всего определяется системой киберпространства. Иными словами, для расследования преступлений, совершенных в киберпространстве, требуются как технические, так и теоретические знания. Соответственно, возникает необходимость выработки единого понятия киберпространства с точки зрения криминалистики.

Что касается назначения компьютерно-технической экспертизы, то здесь надо отметить, что следователям приходится сталкиваться с загруженностью государственных судебно-экспертных учреждений и, как следствие, несвоевременностью выполнения экспертиз.

Другой проблемой при назначении экспертиз является постановка грамотных вопросов эксперту, проводящему компьютерно-техническую экспертизу, что отметили 53 % опрошенных. Назначающие экспертизу связывают возникающие трудности с отсутствием у них практики расследования данной категории дел, сложностью технических терминов и отсутствием специальных знаний в этой сфере.

Решение данной проблемы лежит в плоскости взаимодействия следователя при назначении экспертизы с экспертом или специалистом, которые могут проконсультировать назначающего экспертизу по всем вопросам научно-методического характера.

Таким образом можно сделать вывод, что раскрытие и расследование

мошенничества в сфере компьютерной информации остается довольно сложной задачей для большинства сотрудников органов предварительного расследования. Это отчасти обусловлено отсутствием системных обобщений материалов следственной и судебной практики, нехваткой методических рекомендаций по организации расследования данного вида преступлений, небольшим опытом работы конкретных следователей и работников органов дознания со специфическими источниками доказательственной информации, находящейся в электронной цифровой форме в виде электронных сообщений, страниц, сайтов, а также недостаточно высоким уровнем подготовки следователей по соответствующей специализации в высших учебных заведениях.

Как показало исследование научной литературы и опрос следователей (дознавателей), для решения приведенных проблем и повышения эффективности расследования данных преступлений необходимо: повысить уровень мониторинга данного вида преступлений; разработать программы повышения квалификации следователей (дознавателей) по расследованию данной категории дел; повысить технические возможности экспертов, специализирующихся в области исследования компьютерных технологий; увеличить объем научно-методической литературы, посвященной прикладным аспектам расследования киберпреступлений в целом и мошенничества в сфере компьютерной информации, как одного из видов данных преступлений.

# ЗАКЛЮЧЕНИЕ

Среди всех преступлений против собственности, активно видоизменяющихся в условиях рыночной экономики, особое место принадлежит мошенничеству. Особенность заключается в том, что мошенничество, оставаясь в рамках законодательной трактовки «советских времен», приобрело новые формы, подлежащие доктринальному осмыслению. В теории остается еще множество спорных вопросов толкования признаков данного состава преступления, а на практике уже возникает множество вопросов и трудностей при квалификации деяний и разграничении их со смежными составами.

В связи с изменениями в Закон № 207- ФЗ, внесенными 29.11.2012, существенным образом изменилось правовое регулирование отношений, связанных с вопросами привлечения к уголовной ответственности за мошенничество. Помимо изменений в саму ст. 159 УК РФ, предусматривающую ответственность за мошенничество, глава 21 УК РФ была дополнена шестью новыми статьями (ст.ст. 159.1 - 159.6 УК РФ), предусматривающими уголовную ответственность за различные виды мошенничества:

- мошенничество в сфере кредитования (ст. 159.1);
- мошенничество при получении выплат (ст. 159.2);
- мошенничество с использованием платежных карт (ст. 159.3);
- мошенничество в сфере предпринимательской деятельности (ст.159.4);
- мошенничество в сфере страхования (ст. 159.5);
- мошенничество в сфере компьютерной информации (ст. 159.6).

Что касается мошенничества в сфере компьютерной информации, то криминализация данного вида мошенничества является закономерным шагом интеграции российского законодательства о борьбе с компьютерными преступлениями в международное.

Статья 159.6 УК РФ состоит из четырех частей, первая из которых раскрывает понятие мошенничества в сфере компьютерной информации, 2, 3 и 4

части указанной статьи содержат квалифицированные составы данного преступления по признакам:

- деяния, совершенного группой лиц по предварительному сговору (ч. 2);

- с причинением значительного ущерба гражданину (ч. 2);

- совершения лицом с использованием своего служебного положения (ч. 3);

- совершения в крупном размере (ч. 3);

- совершения организованной группой (ч. 4);

- совершения в особо крупном размере (ч. 4).

Преступление, предусмотренное ч. 1 ст. 159.6 УК РФ является преступлением небольшой степени тяжести, преступления, предусмотренные ч. 2 и 3 ст. 159.6 УК РФ – преступлениями средней тяжести, а преступления, предусмотренные ч. 4 указанной статьи, – отнесены к тяжким.

Объективную сторону мошенничества в сфере компьютерной информации составляет хищение чужого имущества или приобретение права на чужое имущество. Способом совершения преступления выступает: ввод, удаление, блокирование, модификация компьютерной информации; иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно - телекоммуникационных сетей.

Субъект в данном виде мошенничества общий, по ч. 3 ст. 159.6 УК РФ – специальный, квалифицирующими признаками выступает совершение преступления группой лиц по предварительному сговору, либо организованной группой. Субъективная сторона предполагает прямой умысел.

Из диспозиции ст. 159.6 УК РФ следует, что предусмотренное указанной статьей деяние совершается не путем обмана или злоупотребления доверием как все остальные виды мошенничества, а путем использования компьютерной информации.

Общественную опасность мошенничества в сфере компьютерной информации формируют общественно-опасные последствия в виде имущественного

ущерба, причиняемого собственнику или иному владельцу имущества. Мошенничество в сфере компьютерной информации является общественно-опасным именно в силу того, что соответствующие манипуляции с компьютерной информацией выступают в качестве способа хищения чужого имущества или приобретения права на чужое имущество.

При совершении рассматриваемого преступления виновное лицо может совершить одно действие, образующее объективную сторону, либо выполнить несколько действий. Кроме того, преступление, предусмотренное ст. 159.6 УК РФ может быть совершено путем только активных действий.

Согласно данным статистики МВД по Амурской области мошенничество в сфере компьютерной информации становится все более распространенным преступлением. С 2012 года по октябрь 2016 года количество таких преступлений постепенно увеличивается. Так в 2012 году правоохранительными органами не было зарегистрировано ни одного преступления, в 2013 году их количество было так же равно нулю, а вот в 2014 году их количество составило 2, в 2015 году так же 2 преступления о мошенничестве в сфере компьютерной информации в 2016 году эта цифра достигла показателя 3 преступлений.

Так как данная норма была введена законодателем в УК РФ сравнительно недавно, то очевидно возникновение ряда проблем, с которыми сталкиваются отечественные суды и правоохранительные органы при квалификации компьютерного мошенничества.

Анализ судебной практики показал, что основными проблемными вопросами, при квалификации мошенничества в сфере компьютерной информации судами РФ являются:

- рассмотрение обмана, как одного из основополагающих признаков мошенничества. Обман, как способ совершения хищения не характерен для компьютерного мошенничества. Обман выступает не способом изъятия и обращения чужого имущества в пользу виновного, а способом завладения конфиденциальной информацией;

- признание преступления оконченным. При мошенничестве в сфере ком-

пьютерной информации хищение признано оконченным не в момент получения виновным наличных денег, а с момента зачисления их на указанный счет. Если лицо не имело возможности распорядиться похищенным имуществом вследствие того, что, например, расчетный счет в банке, на котором аккумулировались денежные средства, изначально был заблокирован кредитной организацией, то такие случаи буду расценены судом, как покушение на компьютерное мошенничество;

- вопрос о квалификации содеянного, как покушение в ситуациях группового компьютерного мошенничества, когда момент «приобретения лицом реальной возможности распорядиться похищенным» обусловлен совершением действий третьими лицами;

- вопрос определения единого продолжаемое преступления или совокупности преступлений.

Судами мошенничество в сфере компьютерной информации рассматривается как новая форма хищения, как это и предусмотрено законодательством, и большинство криминалистов разделяют данный подход. Однако, Верховному Суду в Постановлении Пленума от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» необходимо пересмотреть позицию в части квалификации таких преступлений, когда совершается хищения из банкомата посредством поддельной платежной карты, признав, что в данном случае совершается не кража, как в большинстве случаев такие преступления квалифицируются, а мошенничество в сфере компьютерной информации.

На территории Российской Федерации борьбу с мошенничеством реализуют в основном органы МВД, отделов по борьбе с экономическими преступлениями УВД. Однако отечественные правоохранительные органы сталкиваются с множеством проблем при расследовании мошенничества в сфере компьютерной информации.

В рамках бакалаврской работы было проведено анкетирование, среди сотрудников следственных отделов и отделов дознания Амурской области. Всего

было опрошено 70 сотрудников различных отделов. В ходе данного исследования были сделаны следующие выводы.

Одной из проблем расследования мошенничества в сфере компьютерной информации является недостаточная компетентность лиц, которые занимаются их выявлением и раскрытием.

Большинство следователей (дознавателей) (86 % респондентов) отметили, что имеющихся знаний для расследования компьютерного мошенничества недостаточно.

Другой проблемой является несвоевременность выявления компьютерного.

Очевидно, что запоздалое начало предварительного расследования может привести к безвозвратной утрате важных доказательств, увеличению сроков предварительного расследования и другим негативным последствиям. Как правило, несвоевременное выявление таких преступлений влечет за собой опасность уничтожения следов их совершения.

При расследовании мошенничества в сфере компьютерной информации чаще всего проводятся такие следственные действия, как осмотр места происшествия (указали 79 % опрошенных), допрос (68 %), обыск (63 %), выемка (37 %) и назначение судебных экспертиз (47 %). Наибольшие трудности возникают при проведении осмотра места происшествия (это отметили 42 % опрошенных) и назначении судебных экспертиз (37 % опрошенных).

Решение данной проблемы лежит в плоскости взаимодействия следователя при назначении экспертизы с экспертом или специалистом, которые могут проконсультировать назначающего экспертизу по всем вопросам научно-методического характера.

Кроме того, для расследования преступлений, совершенных в киберпространстве, требуются как технические, так и теоретические знания.

В целом, раскрытие и расследование мошенничества в сфере компьютерной информации является довольно сложной задачей для большинства сотрудников органов предварительного расследования. Это отчасти обусловлено от-

сутствием системных обобщений материалов следственной и судебной практики, нехваткой методических рекомендаций по организации расследования данного вида преступлений, небольшим опытом работы конкретных следователей и работников органов дознания со специфическими источниками доказательственной информации, находящейся в электронной цифровой форме в виде электронных сообщений, страниц, сайтов, а также недостаточно высоким уровнем подготовки следователей по соответствующей специализации в высших учебных заведениях.

Для решения приведенных проблем и повышения эффективности расследования данных преступлений необходимо: повысить уровень мониторинга данного вида преступлений; разработать программы повышения квалификации следователей (дознавателей) по расследованию данной категории дел; повысить технические возможности экспертов, специализирующихся в области исследования компьютерных технологий; увеличить объем научно-методической литературы, посвященной прикладным аспектам расследования киберпреступлений в целом и мошенничества в сфере компьютерной информации, как одного из видов данных преступлений.

# БИБЛИОГРАФИЧЕСКИЙ СПИСОК

I Правовые акты

1 Конституция Российской Федерации от 12.12.1993 (ред. от 21.07.2014) // Собрание законодательства РФ. – 2014. – № 31. – Ст. 4398.

2 Конвенция совета Европы от 23.11.2001 ETS № 185 «О преступности в сфере компьютерной информации» (в ред. дополнительного протоколом от 28 января 2003 г. ETS № 189) [Электронный ресурс]. – Режим доступа: http:/ /www.consultant.ru/. – 15.09.2016.

3 Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (в ред. от 07 февраля 2017 г.) // Собрание законодательства РФ. - 1996. - № 25. - С. 4578-4689.

4 Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 19.12.2016) (с изм. и доп., вступ. в силу с 01.01.2017) //Собрание законодательства РФ. – 2001. - № 52 (ч. I). - Ст. 4921.

5 Федеральный закон от 29 ноября 2012 г. № 207 - ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» (по состоянию на 03 июля 2016 г.) // Собрание законодательства РФ. – 2012. - № 49. – Ст. 6752.

II Специальная литература

6 Александрова, И.А. Новое уголовное законодательство о мошенничестве / И.А. Александрова // Вестник Нижегородской академии МВД России. - 2013. – № 21. - С. 54-62.

7 Андреев, Б.В. Расследование преступлений в сфере компьютерной информации: учебное пособие / Б.В. Андреев. – М.: МАИК «Наука / Интерпериодика», 2015. – 527 с.

8 Безверхов, А.Б. Развитие понятия мошенничества в отечественном праве / А.Б. Безверхов // Уголовное право.– 2001. - № 4. - С. 8-12.

9 Владимировский – Буданов, М.Ф. Обзор истории русского права: монография / М.Ф. Владимировский - Буданов. – Киев, 2011. - 430 с.

10 Гарбатович, Д.А. Проблемные аспекты эффективности норм, предусматривающих уголовную ответственность за совершение преступлений в сфере компьютерной информации / Д.А. Гарбатович // Библиотека криминалиста. – 2013. – № 5 (10). - С. 40 - 47.

11 Гладких, В.И. Международное сотрудничество в сфере борьбы с компьютерной преступностью: сборник материалов международной научно-практической конференции. / В.И. Гладких. - М.: Международный юридический институт, 2012. – 498 с.

12 Гуров, А.И. Мошенничество и его профилактика / А.И Гуров. - М., 2014. - 450 с.

13 Гузеева, О.С. Действие Уголовного кодекса России в отношении интернет-преступлений / О.С. Гузеева // Законы России: опыт, анализ, практика – 2013. - № 10. - С. 32 - 41.

14 Гульбин, Ю.А. Преступления в сфере компьютерной информации: учебное пособие / Ю.А. Гульбин. – М.: Статут, 2007. – 151 с.

15 Елин, В.М. Мошенничество в сфере компьютерной информации как новый состав преступления / В.М. Елин // Бизнес-информатика. – 2013. - № 2 (24). - С. 70-76.

16 Елисеев, С.А. Преступления против собственности по Уголовному Уложению 1903 г. / С.А. Елисеев [Электронный ресурс]. – Режим доступа: http://law.isu.ru/ru/science/vestnik/index.html. – 10.09.2016.

17 Журавлев, М.А. Актуальные вопросы судебной практики по уголовным делам о мошенничестве / М.А. Журавлев, Е.В. Журавлева // Уголовное право.– 2008. - № 2. – С.95 – 101.

18 Завидов, Б.Д. Обычное мошенничество и мошенничество в сфере высоких технологий / Б. Д. Завидов // Юрист.– 2002. - № 7. – С. 48 – 54.

19 Ильин, И.В. Историческое развитие уголовно-правового понятия мошенничество в Российском законодательстве / И.В. Ильин // История государства и права. – 2007. - № 3. - С.14-17.

20 Кригер, А.И. История мошенничества / А.И. Кригер // Юрист. - 2011. -

№ 10. - С. 41−45.

21 Косых, С.В. Мошенничество и борьба с ним / С.В. Косых. - М., 2011. – 98 с.

22 Колоколов, Н.А. Мошенничество: эффективность уголовно-правового запрета / Н.А. Колоколов // Уголовный процесс. – 2012. - № 5. – С. 115 – 125.

23 Козаев, Н.Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства): монография / Н.Ш. Козаев. - М., 2015. - 257 с.

24 Коржов, В.К. Право и Интернет: теория и практика: учебное пособие / В.К. Коржов. – М.: Издательство БЕК, 2006. – 236 с.

25 Кочои, С.Н. Ответственность за неправомерный доступ к компьютерной информации / С.Н. Кочои. – М.: Изд-во РАГС, 2004. – 221 с.

26 Крылов, В.В. Информация как элемент криминальной деятельности: учебное пособие / В.В. Крылов. – М.: Юрист, 2005. – 440 с.

27 Крылов, В.В. Информационные преступления - новый криминалистический объект: учебное пособие / В. В. Крылов. – М.: Феникс, 2007. – 223 с.

28 Крылов, В.В. Информационные компьютерные преступления: учебное пособие / В.В. Крылов. – М.: Юрид. лит., 2005. – 240 с.

29 Кудрявцев, В.Н. Общая теория квалификации преступлений / В.Н. Кудрявцев. — М., 2012. – 487 с.

30 Лимонов, В.А. Отграничение мошенничества от смежных составов преступления / В.А. Лимонов // Законность. – 2012. - № 3.- С.10-12.

31 Максимов, В.Ю. Компьютерные преступления (вирусный аспект): учебное пособие / В.Ю. Максимов. – М.: АО «Центр ЮрИнфор», 2006. – 210 с.

32 Панфилова, Е.И. Компьютерные преступления: учебное пособие / Е.И. Панфилова. – М.: Феникс, 2007. – 254 с.

33 Решетников, А.Ю. Покушение на преступление в российском уголовном праве: дисс. … канд. юрид. наук / А.Ю. Решетников - М., 2007. – 255 с.

34 Сафонов, О.М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и

правоприменительной практики, перспективы совершенствования: дисс. … канд. юрид. наук / О.М. Сафонов. - М., 2015. – 345 с.

35 Сальников, В.П. Компьютерная преступность: учебное пособие / В.П. Сальников. – М.: Приор, 2014. – 192 с.

36 Симкин, Л.И. Компьютерное пиратство: учебное пособие / Л.И. Симкин. – М.: Статут, 2015. – 499 с.

37 Сухарев, А.А. Компьютерные преступления: учебное пособие / А.А. Сухарев. – М.: Приор, 2008. – 144 с.

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

39 Третьяк, М.Б. Модификация компьютерной информации и ее соотношение с другими способами компьютерного мошенничества / М.Б. Третьяк // Уголовное право. – 2016. - № 2. - С.125-137.

40 Хоменко, С.М. Уголовное право. Особенная часть: учебное пособие / С.М. Хоменко. - М., 2008. – 355 с.

41 Шеслер, А.А. Мошенничество: Проблемы реализации законодательных новелл / А.А. Шеслер // Уголовное право. – 2013. - № 2. - С. 47-53.

42 Шумихин, В.Г. Седьмая форма хищения чужого имущества / В.Г. Шумихин [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/. – 01.11.2016.

43 Щепалов, С.А. Мошенничество – это умышленное причинение имущественного ущерба / С.А. Щепалов // Российская юстиция. – 2003. - № 1.

44 Южин, А.А. Дискуссионные вопросы мошенничества в сфере компьютерной информации / А.А. Южин // Право и кибербезопасность. – 2014. - № 2. - С. 35 - 39.

45 Янин, П.С. Специальные виды мошенничества / П.С. Янин // Законность. – 2015. - № 8. - С. 15 - 19.

III Судебная практика

46 Постановление Пленума Верховного суда РФ от 27 декабря 2007 № 51

«О судебной практике по делам о мошенничестве, присвоении и растрате» (в ред. федерального закона от 29 ноября 2012 г. № 207 - ФЗ) // Российская газета. - 2008. – 12 января.

47 Постановление Президиума Алтайского краевого суда от 03 сентября 2013 г. по делу № 44у224/13 [Электронный ресурс]. – Режим доступа: http://www.co№sulta№t.ru/. – 15.10.2016.

48 Апелляционное определение Московского городского суда от 04 сентября 2013 г. по делу № 10 - 6391 [Электронный ресурс]. – Режим доступа: http://www. justicemaker.ru/primers.php. – 01.11.2016.

49 Приговор суда республики Дагестан по делу № 1 - 28/2013 [Электронный ресурс]. - Режим доступа: http://www.gcourts.ru/case/22900134. – 10.09.2016.

50 Приговор Московского городского суда от 24 апреля 2013 г. по делу № 10 - 2268/2013 [Электронный ресурс]. - Режим доступа: http://www. gcourts.ru/case/ – 10.09.2016.

51 Обзор судебной практики Верховного суда РФ по уголовным делам от 23 декабря 2015 г. № 4 // Бюллетень Верховного Суда РФ. – 2016. - № 9. – С. 153 – 157.

# ПРИЛОЖЕНИЕ А

## АНКЕТА

**Уважаемый респондент! Просим Вас ответить на вопросы данной анкеты. Опрос проводится с целью изучения проблем, возникающих при расследовании мошенничества в сфере компьютерной информации.**

1. Ваша должность?
2. Стаж работы в правоохранительных органах?
3. Приходилось ли Вам заниматься расследованием компьютерных преступлений?

   А) Да  Б) Нет
4. Как часто Вам приходится расследовать преступления связанные с мошенничеством в сфере компьютерной информации?

   А) Часто Б) Никогда не приходилось В) Расследовал от 1 до 5 преступлений
5. Как вы считаете, обладаете ли Вы достаточными знаниями, для расследования уголовных дел о мошенничестве в сфере компьютерной информации?

   А) Да  Б) Нет
6. Какие следственные действия Вы обычно проводите расследуя дела о мошенничестве в сфере компьютерной информации?

   А) Осмотр места происшествия Б) Опрос В) Выемка

   Г) Назначение судебных экспертиз Д) Обыск
7. С какими проблемами Вам приходится сталкиваться в ходе расследования мошенничества в сфере компьютерной информации?

_____
_____
_____
_____

8. Какие меры на Ваш взгляд позволят повысить эффективность расследования преступлений о мошенничестве в сфере компьютерной информации?

_____
_____
_____
_____
_____