

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Юридический институт

Кафедра уголовного права

УТВЕРЖДАЮ
Заведующий кафедрой

А. Н. Тарбагаев
инициалы, фамилия

« » 2021г.

БАКАЛАВРСКАЯ РАБОТА

40.03.01 – Юриспруденция

Проблемы квалификации мошенничества в сфере компьютерной информации (ст. 159⁶ УК РФ)

Руководитель _____ доцент, канд. юрид. наук П. Л. Сурихин
подпись, дата _____ должность, ученая степень инициалы, фамилия

Выпускник _____ К. К. Чупыра
подпись, дата инициалы, фамилия

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	3
ГЛАВА 1. ЮРИДИЧЕСКИЙ АНАЛИЗ ПРИЗНАКОВ СОСТАВА МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИФНОРАМЦИИ	5
1.1 Объективные признаки состава мошенничества в сфере компьютерной информации.....	5
1.2 Субъективные признаки состава мошенничества в сфере компьютерной информации.....	20
1.3 Квалифицирующие признаки состава мошенничества в сфере компьютерной информации	25
ГЛАВА 2. СОВЕРШЕНСТВОВАНИЕ КВАЛИФИКАЦИИ МОШЕННИЧСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИФНОМАЦИИ	38
2.1 Вопросы квалификации мошенничества в сфере компьютерной информации и их решение	38
2.2 Разграничение мошенничества в сфере компьютерной информации с иными составами преступлений	50
ЗАКЛЮЧЕНИЕ	63
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	68

ВВЕДЕНИЕ

Актуальность темы исследования. Мошенничество – одно из самых традиционных составов преступлений, в достаточной мере изученных в науке уголовного права. Однако наше время характеризуется активным и быстрым становлением информационного общества. Высокие технологии стремительно вошли в человеческую деятельность и предопределяют развитие многих областей человеческой жизни. Увеличивающийся рост числа пользователей современных компьютерных технологий не мог не привлечь представителей криминального мира, вместе с собой и новые способы совершения преступлений, ранее неизвестные правоохранительным органам.

В последние годы использование информационно-телекоммуникационных технологий в преступных целях является серьезной проблемой как для правоприменителей, так и для законодателей. Прогрессивный подход к развитию информационно-телекоммуникационных технологий для продвижения устойчивого развития сопровождается новыми угрозами, связанными с киберпреступностью.

Федеральным законом от 29 ноября 2012 года Уголовный кодекс Российской Федерации был дополнен новыми видами мошенничества, в числе одного из них была статья 159⁶ УК РФ – "Мошенничество в сфере компьютерной информации". С точки зрения развития общества, развитие законодательства в сфере компьютерной информации являлось закономерным и обоснованным. Однако выделение такого состава, как мошенничество в сфере компьютерной информации, породило ряд проблем, связанных как с толкованием, так и с применением данной нормы.

Объектом исследования является сфера общественных отношений, которым может быть причинен ущерб посредством мошенничества в сфере компьютерной информации.

Предметом исследования является уголовно-правовая норма, регламентирующая ответственность за мошенничество в сфере

компьютерной информации (ст. 159⁶ УК РФ), юридическая литература, имеющая отношение к этой проблеме. Кроме того, к предмету исследования относятся правоприменительная практика и статистические данные о применении соответствующих норм.

Целью исследования является анализ норм отечественного законодательства о мошенничестве в сфере компьютерной информации.

Задачами исследования являются:

1. Изучение состава мошенничества в сфере компьютерной информации.

2. Анализ вопросов квалификации мошенничества в сфере компьютерной информации.

3. Изучение судебной практики по делам о мошенничестве в сфере компьютерной информации.

4. Изучение смежных с мошенничеством в сфере компьютерной информации составов преступлений, а так же их разграничение.

Методология исследования включает совокупность методов, таких как системный, логико-правовой, сравнительно-правовой, социологический, статистический.

Теоретической основой работы послужили труды ученых-юристов, действующее уголовное законодательство, законы Российской Федерации. Были изучены и проанализированы работы таких ученых как Е. Н. Бархатовой, А. Г. Безверхова, Н. А. Беляева, А. В. Бриллиантова, О. С. Гузеевой, Н. А. Егоровой, О. В. Ермаковой, Г. В. Журавлевой, М. К. Караповича, Е. В. Коноваловой, Н. Н. Кулешовой, В. М. Лебедева, Т. М. Лопатиной, С. А. Петрова, А. И. Рарога, А. Ю. Решетникова, Е. А. Русскевича, М. Д. Фролова, В. В. Хилюты, Е. И. Христофоровой, А. Ю. Чупровой, А. А. Энгельгардта, А. А. Южина, П. С. Яни и др.

ГЛАВА 1. ЮРИДИЧЕСКИЙ АНАЛИЗ ПРИЗНАКОВ СОСТАВА МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

1.1 Объективные признаки состава мошенничества в сфере компьютерной информации

На первом этапе уголовно-правовой характеристики состава преступления, традиционно, предполагается анализ его объекта, то есть характеристика общественных отношений, затрагиваемых в результате причинения вреда. Объект преступления содержит в себе значимость, в первую очередь, потому как помогает определить границы действия нормы, характер общественной опасности содеянного, а так же имеет большую важность в определении значения конструкции состава отдельных преступлений. Под объектом преступления понимается определенный круг общественных отношений, взятых под охрану действующим уголовным законом¹.

Итак, согласно структуре Особенной части УК, норма о мошенничестве в сфере компьютерной информации содержится в главе 21, соответственно, родовым объектом данного преступления являются общественные отношения в сфере экономики, а видовым – общественные отношения, обеспечивающие охрану права собственности. Содержание видового объекта в данных преступлениях совпадает с непосредственным объектом². Соответственно, непосредственным объектом данного преступления является совокупность общественных отношений в сфере собственности. При рассмотрении различной научной литературы по данной

¹ Ревин В. П. Уголовное право России. Общая часть. М., 2016. С. 127.

² Гладких В. И. Уголовное право России. Общая и Особенная части. Новосибирск, 2015. С. 243.

теме можно заметить, что данное понимание содержание объекта преступления является распространенным.

Однако, вместе с тем, имеется и иная точка зрения. Так, В. М. Лебедев считает, что непосредственным объектом мошенничества в сфере компьютерной информации выступают общественные отношения, сложившиеся в сфере электронного документооборота¹.

Так же, распространенной точкой зрения является характеристика состава мошенничества в сфере компьютерной информации как двуобъектоного. Так, например, Г. В. Журавлева и Н. А. Карпова считают непосредственным объектом преступления общественные отношения, связанные с отношениями собственности, а дополнительным – правовые отношения, обеспечивающие информационную безопасность².

По мнению А. Г. Безверхова, дополнительным объектом, в условиях поступательного движения России к постиндустриальному обществу и использования высоких технологий, является безопасность, так как повышается опасность "компьютерного мошенничества"³. Из тех же соображений исходят Н. Н. Кулешова и Е. И. Христофорова⁴.

По мнению Е. В. Коноваловой, основным непосредственным объектом компьютерного мошенничества являются отношения, охраняющие право собственности, а факультативным объектом являются общественные

¹ Лебедев В. М. Комментарий к Уголовному кодексу Российской Федерации. М., 2017.

² Журавлева Г. В. Мошенничество в сфере компьютерной информации: спорные вопросы теории и практики. М., 2017. С. 153.

³ Безверхов А. Г. Мошенничество и его виды: вопросы законодательной регламентации и квалификации. М., 2015. С. 8.

⁴ Кулешова Н. Н. Особенности квалификации мошенничества в сфере компьютерной информации. М., 2018. С. 41-46.

отношения, направленные на защиту компьютерной безопасности¹. Таким образом, Е. В. Коновалова считает, что совершение компьютерного мошенничества может быть не связано с созданием угрозы причинения вреда компьютерной безопасности. С данным мнением солидарен А. А. Южин. Он отмечает, что в качестве основного объекта данного состава преступления выступают отношения, обеспечивающие безопасное хранение, производство, использование или распространение информации и информационных ресурсов, либо их защиты, а в качестве дополнительного объекта следует признавать общественные отношения собственности².

В своем толковании Пленум Верховного Суда Российской Федерации в постановлении от 30 ноября 2017 г. № 48 "О судебной практике по делам о мошенничестве, присвоении и растрате" в п. 20 разъясняет, что особенность компьютерного мошенничества заключается как раз таки в противоправном вмешательстве в нормальный, установленный порядок функционирования средств хранения, обработки и передачи компьютерной информации³. Следует согласиться с М. Д. Фроловым и с тем фактом, что "в данной части речь идет о причинении вреда отношениям по обеспечению безопасности компьютерных данных и систем", что так же указывает на двуобъектность данного вида мошенничества. Такой же точки зрения придерживается и Е. А. Русскевич, а так же отмечает, что в связи с двуобъектностью преступления, по правилам квалификации преступлений, должна исключать совокупность.

¹ Коновалова Е. В. Особенности объекта и предмета преступления, предусмотренного ст. 159⁶ УК РФ. М., 2020. С. 65.

² Южин А. А. Мошенничество и его виды в российском уголовном праве: автореф. дис. ...канд. юрид. наук : 12.00.08. М., 2016. С. 10.

³ Постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 "О судебной практике по делам о мошенничестве, присвоении и растрате".

Однако, совокупность преступлений не исключена ввиду того, что нормы главы 28 УК РФ содержат более строгие санкции¹.

Таким образом, можно сделать вывод, что основным непосредственным объектом мошенничества в сфере компьютерной информации являются охраняемые уголовным законом общественные отношения в сфере собственности. В качестве дополнительного или факультативного объекта выступают общественные отношения, обеспечивающие информационную безопасность.

Переходя к анализу предмета мошенничества в сфере компьютерной информации становится понятно, что мнения ученых расходятся и данный вопрос не является до конца решенным, ведь согласно доктрине, под предметом преступления необходимо понимать исключительно вещь, которая существует в материальном мире, которая представляет материальную ценность для человека и может удовлетворить его потребности. Непосредственно на предмет преступления воздействует преступник в результате своего посягательства².

Как считает Е. В. Коновалова, под предметом в составе мошенничества в сфере компьютерной информации нужно считать альтернативно чужое имущество или приобретение права на чужое имущество³.

Аналогично считают Н. Н. Кулешова и Е. И. Христофорова. Они полагают, что предметом может выступать имущество и право на него⁴.

¹ Русскевич Е. А. Новое постановление Пленума Верховного Суда Российской Федерации о квалификации мошенничества в сфере компьютерной информации. М., 2018. С. 64.

² Игнатов А. Н. Уголовное право России. Учебник для вузов. Т. 1. Общая часть. М., 2000. С. 68.

³ Коновалова Е. В. Особенности объекта и предмета преступления, предусмотренного ст. 159⁶ УК РФ. М., 2020. С. 65.

⁴ Кулешова Н. Н. Особенности квалификации мошенничества в сфере компьютерной информации. Р., 2019. С. 105.

Предметом, по мнению Журавлевой Г. В. и Карповой Н. А., может являться не только чужое имущество и право на чужое имущество, но так же и компьютерная информация, с помощью которой виновный осуществляет обманные действия и завладевает имуществом или приобретает право на имущество¹.

По мнению Н. А. Беляева, в качестве предмета посягательства может выступать каждый из элементов общественного отношения, охраняемого уголовным законом. В качестве предмета преступления могут выступать вещи, физические и юридические лица, их деятельность, даже сам преступник².

Как считаю я, чтобы понять, что является предметом состава мошенничества в сфере компьютерной информации, первоначально нужно понять, что означает само понятие "компьютерной информации". Согласно п. "Б" ст. 1 Соглашения "О сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации" под компьютерной информацией понимается информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи³. Так же, согласно примечанию 1 к ст. 272 УК РФ, компьютерная информация понимается как сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их

¹ Журавлева Г. В. Мошенничество в сфере компьютерной информации: спорные вопросы теории и практики. М., 2017. С. 153.

² Беляев Н. А. Курс советского уголовного права. Часть общая. Ленинград, 1968. С. 303.

³ Федеральный закон от 01.10.2008 № 164-ФЗ. Соглашение "О сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации" .

хранения, обработки и передачи¹. Соответственно, раз это электрические сигналы не ограниченные определенной формой, то можно сделать вывод, что мошенничество заключается в абсолютно не похожих и не унифицированных видах – от банального воровства уникальных сведений из различных носителей информации (стационарного компьютера, телефона, съемного хранилища данных и прочих), в том числе их удаление и изменение, до более сложного, так называемого "фишинга" (то есть выманивание мошенником различных конфиденциальных данных пользователя). По этому, совершенно верно можно определить, что предметом данного состава – мошенничества в сфере компьютерной информации – может являться любая информация (касающаяся личности, банковских карт, бездокументарных ценных бумаг и прочие), имеющая материальную ценность, и, соответственно, это будет являться вещью – имуществом, а так же правом на данное имущество.

Конструкция объективной стороны состава мошенничества в сфере компьютерной информации может характеризоваться следующими признаками: деяние, последствие, причинная связь, время, место, обстановка, орудия, средства, способ. Однако, в современных научных теориях уголовного права нет согласованного понимания о содержании признаков объективной стороны мошенничества в сфере компьютерной информации. Одна из главных тем для дискуссий предполагает вопрос о том, действительно ли компьютерное мошенничество предполагает определенное воздействие на интеллектуальную и волевую сферы потерпевшего для введения его в заблуждение (обман или злоупотребление доверием), так как данный способ является традиционным способом совершения мошенничества по статье 159 УК РФ. Тем не менее, проанализировав и сопоставив составы мошенничества (ст. 159 УК РФ) и мошенничества в сфере

¹ Федеральный закон от 13.06.1996 № 63-ФЗ. Уголовный кодекс Российской Федерации.

компьютерной информации (ст. 159⁶ УК РФ) следует сделать вывод, что компьютерное мошенничество вовсе не предусматривает наличие контакта между лицом, совершающим мошеннические действия с потерпевшим лицом.

По мнению Т. М. Лопатиной, обман или злоупотребление доверием неприменимо к компьютерной системе, которая не имеет интеллекта и воли, а соответственно, не может добровольно передать имущество под влиянием обмана или злоупотребление доверием¹.

Как отмечает А. А. Энгельгардт, для данного вида преступления не характерны: обман человека и передача имущества или приобретение права на имущество с помощью потерпевшего, вызываемые им имущественные последствия являются результатом воздействия виновного лица на компьютерную информацию как средство совершения преступления².

В свою очередь, А. Южин считает аналогичным образом. И отмечает, что вместо обмана и злоупотребления доверием объективная сторона характеризуется такими способами, как ввод, удаление, блокирование, модификация компьютерной информации либо возможно иное вмешательство в информационную сеть, или информационно-телекоммуникационную сеть³.

Подобной позиции придерживается В. В. Хилюта. Он пишет о том, что хищение путем использования компьютерной техники возможно только посредством компьютерных манипуляций. Соответственно, невозможно говорить о том, что при неправомерном злоупотреблении с автоматизированными системами обработки данных присутствует обман.

¹ Лопатина Т. М. Проблемы уголовно-правовой защиты сфер компьютерной информации: современный взгляд на мошенничество. М., 2013. С. 91.

² Энгельгардт А. А. Вопросы квалификации мошенничества в сфере компьютерной информации. М. 2016. С. 86.

³ Южин А. А. Мошенничество и его виды в российском уголовном праве: автореф. дис. ...канд. юрид. наук : 12.00.08. М., 2016. С. 192.

Как пишет автор, обман компьютера – эфемерное понятие, потому что компьютер – это механизм и обмануть его в принципе невозможно. Но возможно взломать или обойти систему защиты¹.

Так же, в теории уголовного права высказывается такая точна зрения, согласно которой наличие обмана или злоупотребление доверием исключает возможность квалификации содеянного по ст. 159⁶ УК РФ. Так, например, некоторыми учеными обосновывается идея того, что если лицо использует смартфон, электронную почту или интернет-магазин, обманывая конкретных потерпевших способом хищения, будет не злоупотребление компьютерной информацией, а обман человека. Такое мошенничество следует квалифицировать по ст. 159, а не по ст. 159⁶ УК РФ².

Так, например, в соответствии с первым пунктом Постановления Пленума Верховного Суда Российской Федерации от 30.11.2017 года № 48 "О судебной практике по делам о мошенничестве, присвоении и растрате", способами хищения чужого имущества или приобретения права на чужое имущество при мошенничестве, ответственность за которое наступает в соответствии со статьями 158¹, 159, 159¹, 159², 159³, 159⁵ УК РФ, являются обман или злоупотребление доверием, под воздействием которых владелец имущества или иное лицо передают имущество или право на него другому лицу либо не препятствуют изъятию этого имущества или приобретению права на него другим лицом³. Таким образом, Верховный Суд Российской Федерации поставил в данном вопросе точку.

Данный признак, об отсутствии в объективной стороне действий, направленных на обман или злоупотребление доверием потерпевшего,

¹ Хилюта, В. В. Хищение с использованием компьютерной техники или компьютерное мошенничество? М., 2013. С. 55.

² Бриллиантов А. В. Комментарий к Уголовному кодексу Российской Федерации (постатейный). М., 2015.

³ Постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 "О судебной практике по делам о мошенничестве, присвоении и растрате".

является принципиальным отличием мошенничества с использованием информационно-телекоммуникационных технологий от мошенничества классического.

Однако, существует практика, согласно которой можно осуществить преступление путем ввода в заблуждение. Так, например, Г. осужден по ч.3 ст. 159⁶ УК РФ. Находясь в помещении торговой точки ЗАО и будучи одетым в форму сотрудника данной организации, и, представившись новым сотрудником ЗАО, введя , таким образом, в заблуждение находящегося на рабочем месте менеджера, путем обмана получил неправомерный доступ к моноблочному персональному компьютеру и путем ввода компьютерной информации в программу 1С, осуществил три перевода денежных средств, принадлежащих Обществу, получив реальную возможность, распорядится похищенными денежными средствами, тем самым, похитив их. После чего, Г., покинул вышеуказанную торговую точку, и, продолжая свои преступный умысел, обналичил в банкомате со своего счета данные денежные средства, тем самым, похитив их¹.

Несмотря на то, что данный состав преступления хоть и является производным от состава мошенничества, однако не может иметь во главе своей конструкции такие признаки как обман или злоупотребление доверием. По мнению Генеральной прокуратуры Российской Федерации, способами совершения мошенничества в сфере компьютерной информации являются:

а) уничтожение информации – это приведение информации или ее части в непригодное для использования состояние независимо от возможности ее восстановления. Уничтожением информации не является переименование файла, где она содержится, а также само по себе автоматическое «вытеснение» старых версий файлов последними по времени;

¹ Приговор Симоновского районного суда Г. Москвы от 14 февраля 2013 г. по делу № 1-79/2013.

б) блокирование информации – результат воздействия на компьютерную информацию или технику, последствием которого является невозможность в течение некоторого времени или постоянно осуществлять требуемые операции над компьютерной информацией полностью или в требуемом режиме, то есть совершение действий, приводящих к ограничению или закрытию доступа к компьютерному оборудованию и находящимся на нем ресурсам, целенаправленное затруднение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением;

в) модификация информации – внесение изменений в компьютерную информацию (или ее параметры). Законом установлены случаи легальной модификации программ (баз данных) лицами, правомерно владеющими этой информацией, а именно: модификация в виде исправления явных ошибок; модификация в виде внесения изменений в программы, базы данных для их функционирования на технических средствах пользователя; модификация в виде частной декомпиляции программы для достижения способности к взаимодействию с другими программами;

г) копирование информации – создание копии имеющейся информации на другом носителе, то есть перенос информации на обособленный носитель при сохранении неизменной первоначальной информации, воспроизведение информации в любой материальной форме – от руки, фотографированием текста с экрана дисплея, а также считывания информации путем любого перехвата информации и т.п.

По мнению А. А. Южина объективная сторона характеризуется такими способами, как:

а) ввод – процесс непосредственного внесения в систему данных информации с носителя, клавиатуры или другого устройства и последующая их запись в информационную систему;

б) удаление – совершение манипуляций, в результате которых информация исчезает с источника хранения;

в) блокирование – создание препятствий к использованию компьютерной информации другим пользователям (сама информация при этом сохраняется);

г) модификация компьютерной информации – изменение содержания или объема информации на ее носителях при обработке ее техническими средствами;

д) иное вмешательство в информационную сеть, или информационно-телекоммуникационную сеть – любое воспрепятствование нормальному процессу функционирования информационной или информационно-телекоммуникационной сети¹.

Как мне кажется, оба списка дополняют друг друга и имеют большое значение в раскрытии способов совершения преступления данного вида.

Так же, исходя из всего выше сказанного, М. Д. Фролов справедливо сделал вывод, что можно определить признаки способа совершения мошенничества в сфере компьютерной информации. Это:

1) действия, совершаемые в виртуальном пространстве посредством использования компьютерной информации;

2) действия, не ориентированные на сознание человека и введение его в заблуждение;

3) манипуляции с компьютерной информацией, сопряженные как с правомерным доступом к компьютерной системе (компьютерной информации), так и без такового;

4) манипуляции с компьютерной информацией, направленные на изъятие чужого имущества или получение права на чужое имущество и причинение имущественного ущерба потерпевшему².

¹ Южин А. А. Мошенничество и его виды в российском уголовном праве: автореф. дис. ...канд. юрид. наук : 12.00.08. М., 2016. С. 191.

² Фролов М. Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации: дис. ...канд. юрид. наук : 12.00.08. М., 2018. С. 78.

Так, например, С., имеющая в силу ранее занимаемой должности навыки работы в программном обеспечении расчетного банковского обслуживания, где содержится информация о счетах и персональных данных клиентов Банка, знающая о порядке работы со счетами и вкладами физических лиц в программном обеспечении Банка, действуя из корыстных побуждений вступила с К. в предварительныйговор на совершение хищения денежных средств, длительное время не истребованных со счетов клиентов Банка и находящихся в распоряжении Банка. Согласно преступной договоренности, С. должна была выбрать клиентов Банка, которые длительное время не пользовались счетами, после чего ввести в программу Банка абонентские номера телефонов, используемые ею и К., с целью получения в дальнейшем доступа к дистанционному банковскому обслуживанию (далее ДБО) счетов выбранных клиентов, зарегистрировать личные кабинеты этим клиентам без их согласия и присутствия для осуществления операций по переводу хранящихся на их счетах денежных средств на счета третьих лиц, с целью последующего их хищения. После чего, С. войдя в досье клиента Ф., содержащее персональные данные клиента, без согласия и присутствия Ф. внесла сведения об абонентском номере, находящемся в пользовании у нее и К., тем самым осуществив модификацию информации и получив сведения о персональных данных клиента, содержащиеся в досье для дальнейшего доступа к ДБО его счетов. Затем С. и К., обладая информацией об открытом Ф. счете произвели операции по переводу денежных средств на счет К. от имени клиента, подтвердив указанные операции путем введения кодов, полученных на абонентский номер, находящийся в пользовании С. и К.¹.

¹ Постановление Советского районного суда г. Красноярска от 18 июня 2019 г. по делу № 1-675/2019.

В дополнение стоит сказать, что данный состав преступления носит материальный характер¹. Преступление окончено с момента наступления хотя бы одного из перечисленных выше последствий неправомерного доступа к конфиденциальной информации или другими словами, с момента появления у виновного реальной возможности распоряжаться похищенным имуществом². Стоит уточнить, что неправомерным будет являться такой доступ к источнику конфиденциальной информации (государственной тайне или доступ лицом, не обладающим необходимыми полномочиями), который будет осуществлен при условии применения специальных мер защиты. Иными словами, неправомерный доступ к компьютерной информации – это незаконное или неразрешенное собственником или иным законным владельцем использование возможности получения компьютерной информации³.

Выбор средства совершения преступления зависит от объекта посягательства, применяемых технических и организационных средств охраны, защиты информации. Преступления совершаются различными способами с применением специальных программно-аппаратных средств и сетевых технологий. Способы совершения компьютерных преступлений становятся высокотехнологичными за счет применения нетривиальных технических решений, а также новых или модифицированных программ.

¹ Кибальник А. Г. Квалификация мошенничества в новом Постановлении Пленума Верховного Суда РФ. М., 2018. С. 65.

² Постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 "О судебной практике по делам о мошенничестве, присвоении и растрате".

³ Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации утв. Генеральной прокуратурой РФ 30.05.2014.

Наличие компьютерных средств является обязательным, именно они предопределяют специфичность способов совершения мошенничества в сфере компьютерной информации¹.

Любое правонарушение причиняет вред общественным отношениям, следовательно, между деянием и наступившими последствиями существует причинная связь. Не существует безвредных правонарушений. И, конечно же, причинно-следственная связь является обязательной в данном составе преступления.

Устанавливая причинную связь между несанкционированным доступом и наступлением вредных последствий следует иметь в виду, что в компьютерных системах возможны уничтожение, блокирование и модификация компьютерной информации в результате технических неисправностей или ошибок при функционировании операционной среды или иных программ. В этих случаях лицо, совершившее неправомерный доступ к компьютерной информации, не подлежит ответственности по данной статье ввиду отсутствия причинной связи между его действиями и наступившими последствиями².

Подводя итог, стоит отметить, что:

- 1) мошенничество в сфере компьютерной информации имеет такой непосредственный объект, как охраняемые законом отношения в сфере собственности. Дополнительный, факультативный объект – охраняемые законом общественные отношения, касающиеся информационной безопасности;
- 2) предметом мошенничества в сфере компьютерной информации выступает имущество и право на имущество – электронные, безналичные

¹ Еремеева А. Д. К вопросу о способах совершения мошенничества в сфере компьютерной информации. Д., 2020. С. 154-157.

² Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации утв. Генеральной прокуратурой РФ 30.05.2014.

деньги, бездокументарные ценные бумаги, цифровые финансовые активы, виртуальные объекты имущества (приобретаемое за реальные деньги и обладающее финансовой ценностью), а так же персональная информация потерпевшего;

3) мошенничество в сфере компьютерной информации по конструкции является материальным составом. Считается оконченным с момента, когда имущество поступило в незаконное владение лица и когда оно получило реальную возможность распоряжаться и пользоваться по своему усмотрению данным имуществом;

4) способами совершения мошенничества в сфере компьютерной информации являются действия, связанные с вводом, удалением, блокированием, модификацией компьютерной информации, а так же вмешательство в функционирование средств хранения, обработки, передачи компьютерной информации, а так же вмешательство в функционирование информационно-телекоммуникационных сетей. К тому же, к способам совершения мошенничества в сфере компьютерной информации может относиться обман или злоупотребление доверием, однако, данный признак не является характерным, как правило, данное преступление не предусматривает наличие контакта между лицом, совершающим мошеннические действия с потерпевшим лицом. Данные действия совершаются для воздействия на компьютерную информацию, а обман или злоупотребление доверием, в исключительных случаях, служат способами достижения получения доступа к компьютеру и информационной системе.

1.2 Субъективные признаки состава мошенничества в сфере компьютерной информации

Традиционно рассмотрение субъективных признаков состава преступления, в нашем случае мошенничества в сфере компьютерной информации, начинается с анализа признаков субъекта, включающая возраст, вменяемость и различные специфические особенности преступника, а так же субъективной стороны, содержащая в своем смысле вину, мотив и цель, предусмотренного ст. 159⁶ УК РФ.

В классическом понимании, субъектом преступления является лицо, совершившее преступление. Из всех многочисленных свойств личности лица, совершившего преступление, необходимо выявить такие, которые указывают на его способность нести уголовную ответственность¹. Именно эти свойства характеризуют субъекта преступления и составляют его признаки.

В качестве субъекта может выступать лицо, обладающее всеми данными признаками. И, согласно статье 19 УК РФ, это должно быть лицо: физическое, вменяемое и достигшее возраста, с которого уголовный закон связывает возможность наступления уголовной ответственности за конкретный вид преступления. При этом, субъектом может быть как гражданин Российской Федерации, так и иностранный гражданин, а так же лицо без гражданства. Отсутствие хотя бы одного из трех указанных законом признаков исключает наличие состава преступления у данного лица.

Определение субъекта мошенничества в сфере компьютерной информации не вызывает дискуссий в науке. Соответственно, можно безошибочно сказать, что субъектом преступления, предусмотренного частями 1, 2 статьи 159⁶ УК РФ (за исключением части 3 ст. 159⁶ УК РФ, так как она имеет квалифицированный вид), является общий субъект, иначе

¹ Плотников А. И. Уголовное право России. Общая часть: Учебник. Оренбург, 2016. С. 120.

говоря, представляет собой вменяемое физическое лицо, и к моменту совершения преступления, достигшее шестнадцатилетнего возраста¹.

По результатам проведенного исследования А. Э. Побегайло, из 100 человек, совершивших компьютерные преступления, 77 преступников имеют средний уровень интеллектуального развития, 21 преступник выше среднего, 2 – ниже среднего. При этом у 20 преступников из 100 образование среднее, у 20 – среднеспециальное, а у 60 – высшее².

Не смотря на то, что в доктрине нет возражений по определению субъекта преступления, есть предложения о необходимости понижения возраста уголовной ответственности за мошенничество в сфере компьютерной информации.

Многие ученые солидарны с С. С. Медведевым и предлагают понизить возраст наступления уголовной ответственности за мошенничество до 14 лет, в основном аргументируя тем, что процесс социализации в данное время значительно ускорен, а так же, что у субъекта данного вида мошенничества нет необходимости иметь визуальный контакт с потенциальной жертвой³.

Переходя к анализу субъективной стороны хочется еще раз отметить, что ее характеристиками являются вина (как обязательный признак), мотив, цель и эмоциональное состояние (как факультативные признаки).

В доктрине уголовного права считается общепринятым мнение о том, что субъективная сторона преступления, предусмотренного ст. 159⁶ УК РФ, относится к категории умышленного в виде прямого умысла. Однако некоторые ученые признают возможность совершения мошенничества в сфере компьютерной информации как с прямым умыслом, так и с

¹ Капинус О. С. Уголовное право России. Общая часть : учебник для бакалавриата, специалитета и магистратуры. М., 2019. С. 193.

² Побегайло А. Э. Киберпреступность: учебное пособие для бакалавров. М., 2014. С. 60.

³ Медведев С. С. Мошенничество в сфере высоких технологий: автореф. дис. ...канд. юрид. наук : 12.00.08. Краснодар, 2008. С. 15.

косвенным. Впрочем данная теория подвергается сомнению подавляющего большинства профессоров. И, например, А. И. Рарог делает замечание о том, что допущение преступлений при наличии любого из видов умысла является следствием применения законодательной конструкции умысла ко всем преступлениям с материальным составом¹.

Как и другие формы хищения, мошенничество в сфере компьютерной информации предполагает наличие корыстной цели, что подразумевает под собой реальный факт волевого желания виновного лица в наступлении общественно опасных последствий, выражющиеся в виде причинения имущественного ущерба потерпевшему лицу².

Интеллектуальный момент наличия прямого умысла при мошенничестве в сфере компьютерной информации выражается в осознании виновным лицом противоправного характера и степень общественной опасности совершенного деяния, а так же выражается в том, что виновный предвидит неизбежность наступления общественно опасных последствий в виде имущественного ущерба потерпевшему как результат неправомерной обработки данных³. Кроме того, обязательно присутствие признаков объективной стороны, с помощью которых совершается преступление.

Одновременно с этим, обязательным признаком мошенничества в сфере компьютерной информации является корыстный мотив преступления.

В соответствии с пунктом 26 Постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 № 48 "О судебной практике по делам о мошенничестве, присвоении и растрате" при решении вопроса о виновности лица, совершившего преступления – мошенничество, присвоение

¹ Рарог А. И. Проблемы квалификации преступлений по субъективным признакам: монография. М., 2015. С. 77.

² Лихолетов, А. А. Проблемы разграничения мошенничества с использованием платежных карт с другими составами преступлений. М., 2017. С. 36.

³ Шеслер, А. В. Содержание умысла по действующему российскому уголовному законодательству. В., 2017. С. 136.

или растрату, суды должны иметь ввиду, что обязательным признаком хищения является наличие у лица корыстной цели, то есть желание и стремление изъять и (или) обратить чужое имущество в свою пользу либо распорядиться указанным имуществом как своим собственным, в том числе путем передачи его в обладание других лиц, круг которых не ограничен¹. Это говорит о том, что корыстный мотив может заключаться не только в своем личном обогащении, но и обогащении близких лиц преступника за счет похищенного имущества, так и других лиц, например, соучастников.

В качестве пример можно привести преступника, который совершает мошенничество в сфере компьютерной информации, мотивируя тем, что "отбирает у богатых и отдает бедным". Данный случай, хоть и не типичен, но не исключает корыстную цель. И такой мотив не является исключением вменения в вину данного состава преступления, если в его деяниях присутствуют обязательные признаки наличия состава преступления, предусмотренного ст. 159⁶ УК РФ.

По мнению С. А. Петрова корыстный мотив следует понимать следующим образом – стремление виновного противоправным путем получить реальную возможность владеть, пользоваться и распоряжаться чужим имуществом как своим собственным, а равно незаконно извлекать иные выгоды имущественного характера не только для себя, но и для других лиц, в том числе посторонних для виновного².

К части третьей ст. 159⁶ УК РФ применяются все те же особенности субъективной стороны преступления, за исключением субъекта указанного преступления. А все потому что в данной части есть квалифицирующий признак – совершение деяния, предусмотренного частями 1, 2 ст. 159⁶ УК

¹Постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 "О судебной практике по делам о мошенничестве, присвоении и растрате".

² Петров С. А. Хищение чужого имущества или приобретение права на него путем обмана: уголовно-правовая оценка и совершенствование правовой регламентации : автореф. дис. ...канд. юрид. наук : 12.00.08. М., 2015. С. 26.

РФ, с использованием лицом своего служебного положения. Этот признак мы рассмотрим чуть позже.

Подводя итог, стоит отметить, что:

1) субъектом мошенничества в сфере компьютерной информации является вменяемое физическое лицо, достигшее шестнадцатилетнего возраста на момент совершения деяния;

2) совершая преступление лицо осознает общественную опасность, предвидит неизбежность наступления последствий и желает их наступления. Соответственно, субъективная сторона мошенничества в сфере компьютерной информации характеризуется умышленной формой вины с прямым умыслом. Виновный преследует корыстную цель, вне зависимости от его мотива.

1.3 Квалифицирующие признаки состава мошенничества в сфере компьютерной информации

Квалифицирующие признаки состава преступления представляют повышенную общественную опасность, поэтому данный вопрос имеет значительный вес в науке и практике.

В составе мошенничества в сфере компьютерной информации совокупностью законодатель предусматривает наличие отягчающих или квалифицирующих признаков. Итак, в составе ст. 159⁶ УК РФ были выделены следующие квалифицирующие признаки:

- деяние по части 1 ст. 159⁶ УК РФ, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину (по части 2);
- деяние, предусмотренное частью 1 или частью 2 ст. 159⁶ УК РФ, совершенное лицом с использованием своего служебного положения (по пункту "А", части 3);
- деяние, предусмотренное частью 1 или частью 2 ст. 159⁶ УК РФ, совершенное в крупном размере (пункт "Б", часть 3);
- деяние, предусмотренное частью 1 или частью 2 ст. 159⁶ УК РФ, совершенное с банковского счета, а равно в отношении электронных денежных средств (пункт "В", часть 3);
- деяние, предусмотренное частью 1, частью 2 или частью 3 ст. 159⁶ УК РФ, совершенное организованной группой либо в особо крупном размере (по части 4).

Отягчающие признаки рассматриваемого преступления схожи с квалифицирующими признаками других форм хищения.

Стоит начать с рассмотрения такого квалифицирующего признака как "деяние, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину".

Итак, согласно ч. 2 ст. 35 УК РФ, преступление признается совершенным группой лиц по предварительному сговору, если в нем

участвовали лица, заранее договорившиеся о совместном совершении преступления, при этом, для того, чтобы преступление было признано таковым должно быть установлено не менее двух соисполнителей, а так же взаимная осведомленность и согласованность между ними, единый умысел, кроме того, характер взаимоотношений между соисполнителями должен быть направлен на достижение общего результата – завладение имуществом потерпевшего¹. Дополнительно, при данном характере отношений, так же важно выполнение каждым соисполнителем своей роли.

Применительно к составу ст. 159⁶ УК РФ, групповой характер совершения мошенничества в сфере компьютерной информации может заключаться в осуществлении одним соисполнителем блокировании информации на компьютере, а другим – в любом ином вмешательстве в функционировании информационно-телекоммуникационной сети. А так же, согласно пункту 10 Постановления Пленума Верховного Суда Российской Федерации от 27 декабря 2002 г. № 29 "О судебной практике по делам о краже, грабеже и разбое", "уголовная ответственность за хищение, совершенное группой лиц по предварительному сговору наступает и в тех случаях, когда, согласно предварительной договоренности между соучастниками, непосредственное изъятие имущества осуществляет один из них. И если другие участники в соответствии с распределением ролей совершили согласованные действия, направленные на оказание непосредственного содействия исполнителю в совершении преступления, то содеянное ими является соисполнительством и в силу части 2 ст. 34 УК РФ не требует дополнительной квалификации по статье 33 УК РФ"².

¹ Подвойкина И. А. Уголовное право в 2 т. Т. 1. Общая часть : учебник для бакалавров. М., 2014. С. 260.

² Постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2002 г. № 29 "О судебной практике по делам о краже, грабеже и разбое".

Участие в мошенничестве по ст. 159⁶ УК РФ лиц, не подлежащих уголовной ответственности в силу возраста или отсутствия вины исключает оценку содеянного по признаку совершения преступления группой лиц по предварительному сговору.

Современная правоприменительная практика показывает, что установление признака значительного ущерба зачастую определяется путем сложения сумм денежных средств, полученных в результате совершения лицом ряда тождественных действий по противоправному изъятию имущества¹.

Конечно же стоит отметить, что данный признак несет за собой оценочный характер, минимальный размер ущерба 2500 рублей (согласно ст. 7.27 КоАП РФ), а максимальный – не должен превышать двухсот пятидесяти тысяч рублей.

Так же, согласно пункту 31 Постановлению Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 "О судебной практике по делам о мошенничестве, присвоении и растрате" при решении вопроса о наличии в действиях квалифицирующего признака причинения гражданину значительного ущерба судам, наряду со стоимостью похищенного имущества, надлежит учитывать имущественное положение потерпевшего, в частности наличие у него источника доходов, их размер и периодичность поступления, наличие у потерпевшего иждивенцев, совокупный доход членов семьи, с которыми он ведет совместное хозяйство. Мнение потерпевшего о значительности или незначительности ущерба, причиненного ему в результате преступления, должно оцениваться судом в

¹ Фролов М. Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации: дис. ...канд. юрид. наук : 12.00.08. М., 2018. С. 107.

совокупности с материалами дела, подтверждающими стоимость похищенного имущества и имущественное положение потерпевшего¹.

Так, например, к уголовной ответственности по ч. 2 ст. 159⁶ УК РФ привлечен И., использовавший персональный компьютер, который был подключен к сети "Интернет", с личного электронного счета Р. в системе "Единый кошелек" путем перечисления на счет платежной системы "Киви-кошелек" похитил денежные средства в сумме 5560 рублей 60 копеек, после чего перечислил данную сумму на свой банковский счет в ОАО "Экспресс-банк" и обналичил посредством снятия через банкомат, причинив таким образом ущерб потерпевшему Р.².

Так же, Г., будучи осведомлен о механизме перевода денежных средств с банковских карт клиентов ПАО «С.», путем удаленного доступа через сеть "Интернет", с помощью системы дистанционного банковского обслуживания «Банк-онлайн» решил совершить мошенничество в сфере компьютерной информации. Действуя с преступным умыслом, для достижения желаемого преступного результата следующую схему мошенничества в сфере компьютерной информации: в ночное время отыскать в мусорных корзинах, стоящих рядом с банкоматами ПАО «С.», чек-идентификатор и чек с одноразовыми паролями, используя которые путем удаленного доступа через сеть «Интернет» с помощью системы дистанционного банковского обслуживания «Банк-онлайн» незаконно проникнуть в «личный кабинет» клиента ПАО «С.», расположенный на сайте ПАО, для получения возможности распоряжаться денежными средствами, находящимися на счете его банковской карты, после чего с помощью электронных поручений осуществить переводы с этого счета денежных средств на счет имеющейся у

¹ Постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 "О судебной практике по делам о мошенничестве, присвоении и растрате".

² Приговор Каспийского городского суда от 26 июня 2013 года по делу № 1-130/2013.

него в распоряжении банковской карты. Получив реальную возможность распоряжаться похищенными при указанных выше обстоятельствах денежными средствами, зачисленными на счет имеющейся у него в распоряжении банковской карты, обратить их в свою пользу. Приступив к реализации преступного умысла, направленного на хищение чужого имущества путем ввода компьютерной информации в функционирование средств хранения, обработки и передачи компьютерной информации, Г., под предлогом отсутствия у него банковской карты и необходимости получения денежных средств, попросил у ранее знакомого К. в пользование принадлежащую последнему банковскую карту. Неосведомленный о преступных намерениях Г. К. согласился и предоставил Г. свою банковскую карту. Продолжая реализовывать преступный умысел Г. незаконно получил чек-идентификатор и чек с одноразовыми паролями для входа в систему дистанционного банковского обслуживания «Банк-онлайн». После чего, Г., используя ранее незаконно полученные им чек-идентификатор и чек с одноразовыми паролями, путем удаленного доступа через сеть «Интернет» с помощью системы дистанционного банковского обслуживания «Банк-онлайн» незаконно проник в «личный кабинет» Б., находящийся на сайте ПАО «С.», где размещалась информация о денежных средствах, находящихся на счете банковской карты, эмитированной Б. ПАО «С.», и, путем ввода компьютерной информации в функционирование средств хранения, обработки и передачи компьютерной информации, осуществил 14 переводов денежных средств на счет банковской карты К., в результате чего Г. получил реальную возможность распоряжаться денежными средствами, похищенными у Б. В результате вышеописанных преступных действий Г. причинил Б. значительный ущерб¹.

¹ Приговор Промышленного районного суда г. Самара Самарской области от 4 октября 2016 г. по делу № 1-206/2016.

По части 3 ст. 159⁶ УК РФ квалифицирующими признаками признается совершение компьютерного мошенничества: лицом с использованием своего служебного положения, в крупном размере, с банковского счета, а равно в отношении электронных денежных средств.

Данный признак в современном Уголовном кодексе РФ, а также судебной практике признается довольно распространенным. Так, например, в практике по делам о мошенничестве в сфере компьютерной информации чаще всего признаются бухгалтера, как лица, использующие свое служебное положение. Однако, в доктрине уголовного права вопрос о толковании данного квалифицирующего признака нельзя назвать до конца решенным. И Н. А. Лопашенко совершенно верно отмечает, что невозможно до бесконечности расширять круг лиц, использующих свое служебное положение¹.

Так, согласно пункту 29 Постановлению Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 "О судебной практике по делам о мошенничестве, присвоении и растрате" под лицами, использующими свое служебное положение при совершении мошенничества в сфере компьютерной информации, следует понимать должностных лиц, обладающих признаками, предусмотренными пунктом 1 примечаний к статье 285 УК РФ, государственных или муниципальных служащих, не являющихся должностными лицами, а также иных лиц, отвечающих требованиям, предусмотренным пунктом 1 примечаний к статье 201 УК РФ (например, лицо, которое использует для совершения хищения чужого имущества свои служебные полномочия, включающие организационно-распорядительные или административно-хозяйственные обязанности в коммерческой организации)².

¹ Лопашенко Н. А. Посягательства на собственность. М., 2012. С. 503.

² Постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 "О судебной практике по делам о мошенничестве, присвоении и растрате".

Представляется, что под полномочиями по распоряжению и управлению имуществом в учреждении или организации следует понимать переданную возможность лицу для принятия самостоятельного решения вопроса о судьбе чужой собственности. А обязанность лица производить перемещение чужого имущества техническим методом (например, работа водителем) не означает наличия у него права по распоряжению или управлению имуществом.

Так, например, гражданка М. была признана виновной в совершении преступления, предусмотренного п. "А", ч. 3 ст. 159⁶ УК РФ. Занимая должность специалиста по сопровождению корпоративных клиентов ПАО, М. используя свое служебное положение, путем модификации компьютерной информации в информационно-биллинговой системе ПАО незаконно осуществила перевод денежных средств, принадлежащих ПАО, со счета Муниципального управления МВД России на свой лицевой счет. В результате гражданка похитила денежные средства¹.

Так же, в науке распространено мнение, заключающееся в том, чтобы расширить характеристику субъекта, использующего свое служебное положение. Например, Н. А. Егорова предлагает расширить понятие до "иных служащих организаций вне зависимости от формы собственности"². Более, чем справедливая мысль. Соглашусь с мнением автора, ведь не только лица, перечисленные в примечании 1 к статье 201 УК РФ имеют доступ к различного толка информации и при этом выполняю установленную трудовую функцию и при этом отвечают за обеспечение информационной безопасности.

¹ Приговор Фрунзенского районного суда г. Саратова от 19 июля 2018 г. по делу № 1-66/2018.

² Егорова Н. А. Ответственность за служебные мошенничества: необходимость нового подхода. М, 2014. С. 20.

Стоит отметить, что крупный размер стоимости имущества должен превышать двести пятьдесят тысяч рублей, но не более миллиона рублей. Размер украденного имущества имеет важное значение. В первую очередь, для оценки степени общественной опасности хищения, в том числе мошенничества в сфере компьютерных технологий.

Существует дискуссионный вопрос, который касается оценки размера похищенного имущества, хранящегося в иностранной валюте. По общему правилу стоимость определяется на момент совершения преступления и исходя из его фактической стоимости, то есть по официальному курсу Центрального Банка Российской Федерации на момент (в данном случае на конкретные число, месяц и год, в некоторых случаях и время) осуществления преступления, то есть на момент, когда была произведена конкретная манипуляция с компьютерной информацией¹. Данный подход распространяется и на другие имущественные объекты, например, на бездокументарные ценные бумаги. Соответственно, дальнейшее изменение котировок акций или изменения на финансовой бирже с национальной валютой не должны влиять и учитываться при квалификации данного преступления.

Включение такого пункта, как "с банковского счета, а равно в отношении электронных денежных средств", как считают ученые, противоречит природе уголовно-правовой нормы об ответственности за данный вид мошенничества. Такое мнение сложилось из-за того, что мошенничество в сфере компьютерной информации изначально даже не предполагало возможности осуществления противоправных действий в отношении бумажных денег. Так как в практике сложилось понимание, того что компьютерное мошенничество так или иначе связано с посягательством

¹ Фролов М. Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации: дис. ...канд. юрид. наук : 12.00.08. М., 2018. С. 114.

именно на безналичные или электронные деньги. Многие ученые призывают исключить данный квалифицирующий признак, так как с его введением законодатель по сути аннулировал действие первой и второй частей данной нормы¹. Однако, мошенничество в сфере компьютерной информации так же будет иметь место в случаях, когда посредством неправомерного вмешательства в функционирование и работу программного обеспечения банкомата, будет осуществляться хищение наличных денежных средств.

Так, например, Е., работая в должности ведущего специалиста операционного отдела отделения банка "В". И имея согласно своих служебных полномочий доступ к автоматизированному программному обеспечению ОАО, в котором отображаются все банковские операции с физическими лицами и формируются электронные платежные поручения, а так же обладая сведениями об одобренных банком кредитах, предоставленных физическим лицам, по которым последними поданы заявления о закрытии счетов, разработала план совершения преступления, согласно которого она (Е.) путем ввода в данную систему не соответствующей действительности компьютерной информации, намеревалась списывать принадлежащие ОАО денежные средства с карточных счетов граждан на свой счет, похищая их таким образом. Реализуя свой преступный умысел, Е., используя свое служебное положение, имея бесконтрольный доступ к автоматизированному программному обеспечению ОАО, находясь на своем рабочем месте, обладая достоверной информацией об одобренных банком кредитах, предоставленных физическим лицам, по которым последними поданы заявления о закрытии счетов, используя свой служебный компьютер, персональную учетную запись (логин и пароль) для доступа в автоматизированное программное обеспечение, вопреки должностным обязанностям, вводила в систему недостоверную

¹ Русскевич Е. А. Новые нормы УК РФ об электронном мошенничестве и коррупционных преступлениях. М., 2018. С. 32.

компьютерную информацию, а именно формировала и отправляла на исполнение заведомо для нее подложные платежные поручения, согласно которым со счетов клиентов ОАО на счет Е. переводились принадлежащие указанному банку денежные средства, которые она похищала и распоряжалась по своему усмотрению. Таким образом, Е. используя свое служебное положение, путем ввода заведомо ложной компьютерной информации, совершила хищение принадлежащих ОАО денежных средств¹.

Согласно части 4 ст. 159⁶ УК РФ, законодатель выделил такие признаки, как совершение мошенничества в составе организованной группы, а равно в особо крупном размере.

Как известно, принципиальным отличием организованной группы от группы лиц по предварительному сговору является более сложная внутренняя организация – устойчивость организованной группы (о чем говорит стабильность состава участников, распределение ролей между ними, подготовка и наличие организатора), а так же целью является совершение одного или нескольких тяжких или особо тяжких преступлений². Важным является то, что данные признаки организованной группы должны быть определяющими при квалификации преступления, предусмотренного ч. 4 ст. 159⁶ УК РФ.

С учетом вышеизложенного, нужно определить, что мошенничество в сфере компьютерной информации стоит считать совершенным организованной группой, если указанные действия осуществлены устойчивой группой лиц, заранее определившихся и подготовившихся для совершения одного или нескольких преступлений.

¹ Приговор Замоскворецкого районного суда г. Москвы от 6 февраля 2015 г. по делу № 1-52/2015.

² Прозументов Л. М. Организованная группа как форма соучастия в преступлении в действующем российском законодательстве. Томск, 2015. С. 67.

Применительно к ч. 4 ст. 159⁶ УК РФ крупный размер должен превышать один миллион рублей. Так же, стоит отметить, что трудности, которые были описаны выше, касаемо крупного размера по п. "В", ч. 3, ст. 159⁶ УК РФ. Пленум в данной части пояснил, что в случае совершения нескольких хищений чужого имущества, общая стоимость которого образует крупный или особо крупный размер, содеянное следует квалифицировать с учетом соответствующего признака, если эти хищения совершены одним способом и при обстоятельствах, свидетельствующих об умысле совершить хищение в крупном и особо крупном размере¹.

Так, например, органами предварительного следствия установлено, что М., Д., Б. умышленно, в составе организованной группы под руководством неустановленных лиц, занимающихся хищением денежных средств путем ввода вредоносной программы и модификации компьютерной информации в банковской электронной системе, с целью тайного хищения денежных средств. В период с 15 июля по 16 июля 2017 года, координируя свои действия с неустановленным лицом посредством соединения по приложению «Т.», с 8 банкоматов, принадлежащих АКБ «Б.» похитили денежные средства, выдаваемые банкоматами, которыми в результате ввода вредоносной программы и модификации компьютерной информации в банковской электронной системе АКБ «Б.» путем удаленного доступа управляли неустановленные лица, на общую сумму не менее миллиона рублей².

Так же, например, Б., являясь ведущим специалистом Отдела развития Управления процессинга и технологий банка, имея умысел на мошенничество в сфере компьютерной информации, путём ввода,

¹ Постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 "О судебной практике по делам о мошенничестве, присвоении и растрате".

² Апелляционное постановление Верховного Суда Республики Саха (Якутия) от 26 октября 2017 г. по делу № 22К-1671/2017.

модификации компьютерной информации, имея доступ к компьютерным системам указанного банка, находясь в офисе, используя рабочий компьютер, ввел свои логин и пароль, позволяющие ему войти в систему «Online», то есть компьютерную программу, позволяющую изменять данные и значения расчётных счетов. В тот же день, Б., путём ввода компьютерной информации, произвел модификацию компьютерной информации, увеличил доступный остаток на принадлежащем ему счёте с 0 на 6 379 363 рубля, то есть приобрёл право на принадлежащие Банку, денежные средства на указанную сумму, то есть в особо крупном размере. С этого момента он получил право на данные денежные средства, получив реальную возможность пользоваться и распоряжаться ими по своему усмотрению. Продолжая реализацию преступного умысла Б. уволился из Банка. После указанного выше неправомерного изменения доступного остатка на счете он осуществил несколько внешних банковских переводов с принадлежащего ему расчётного счета на подконтрольные ему расчётные счёта открытые в ЗАО КБ, в дальнейшем указанные средства снял. Таким образом, Б. совершил мошенничество в сфере компьютерной информации, то есть хищение чужого имущества и приобретение права на принадлежащие Банку, путем ввода, модификации компьютерной информации, в особо крупном размере¹.

Подводя итог, стоит отметить, что:

1) такой признак как значительный ущерб носит оценочный характер, минимальный размер которого установлен в ст. 7.27 КоАП РФ и составляет не более 2500 рублей, а максимальный размер ущерба не должен превышать двухсот пятидесяти тысяч рублей. Крупный размер не должен превышать миллиона рублей, а особо крупный превышает миллион рублей;

2) групповой характер совершения мошенничества в сфере компьютерной информации может заключаться в осуществлении

¹ Приговор Хорошевского районного суда г. Москвы от 28 ноября 2014 г. по делу № 1-585/2014.

соисполнителями разных функций или способов совершения преступления, например, одним соисполнителем – блокирование информации на компьютере, а другим может заключаться в любом ином вмешательстве в функционировании информационно-телекоммуникационной сети;

3) такой признак, как совершение преступления лицом с использованием своего служебного положения имеет отношение к лицам, приведенным в примечании к ст. 285 УК РФ и ст. 201 УК РФ;

4) признак организованной группы в ч. 4 ст. 159⁶ УК РФ вступает в силу, если указанные действия совершены устойчивой группой лиц, которые заранее объединились и подготовились к совершению одного или нескольких преступлений.

ГЛАВА 2. СОВЕРШЕНСТВОВАНИЕ КВАЛИФИКАЦИИ МОШЕННИЧСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИФНОМАЦИИ

2.1 Вопросы квалификации мошенничества в сфере компьютерной информации и их решение

Проблема квалификации преступлений является преимущественным вопросом для практики как расследования преступления, так и суда, а так же наиболее сложным. При квалификации преступления дается юридическая оценка действиям и обстоятельствам, содержащим признаки состава преступления, предусмотренных уголовным законом.

Квалификация преступлений осуществляется компетентными государственными органами, например, на предварительном следствии или в судебном заседании при рассмотрении дела. Итоговая квалификация закрепляется в различных правоприменительных актах, например, в обвинительном заключении, приговоре суда и т.д.

Процесс квалификации преступлений принято делить на три этапа. Во-первых, необходимо правильно и полно установить фактические обстоятельства совершенного деяния, имеющие значение для квалификации. Во-вторых, устанавливается уголовно-правовая норма, описывающая соответствующий состав преступления. В-третьих, сопоставляются фактические обстоятельства с признаками, характеризующими объект и объективную сторону преступления, затем субъект и субъективную сторону преступления. В отдельных случаях данные обстоятельства конкретного деяния одновременно сопоставляются с признаками нескольких составов преступлений¹.

¹ Карапович М. К. Квалификация преступлений: понятие, особенности и проблемы. М., 2014. С. 161.

В отношении состава мошенничества в сфере компьютерной информации у правоприменителей отсутствуют четкие правила квалификации. Правоприменительная практика и научная литература по данному вопросу предоставляет возможность сделать вывод о том, что многие вопросы по оценке компьютерного мошенничества до сих пор остаются нерешенными.

Так, например, не исключается, что мошенничество в сфере компьютерной информации может совершаться на территории нескольких государств. В данном вопросе отсутствует определенность – территорию какой страны следует признавать местом совершения преступления: место расположения технических устройств; местонахождение лиц, совершивших деяние или место наступления общественно опасных последствий преступления. Существует мнение, что адрес сайта не означает, что какой-либо сайт ведет деятельность в соответствующей стране¹.

На взгляд М. Д. Фролова, местом совершения мошенничества в сфере компьютерной информации следует считать территорию того государства, где было совершено общественно опасное деяние, независимо от того, где наступили общественно опасные последствия. Кроме того, преступление, предусмотренное ст. 159⁶ УК РФ, следует считать совершенным на территории Российской Федерации, если оно начинается на территории другого государства (иными словами, там, где осуществилась организаторская деятельность, подстрекательство либо пособничество), а оканчивается на территории Российской Федерации².

Так же, остается дискуссионным вопрос о квалификации мошенничества в сфере компьютерной информации как неоконченного

¹ Гузеева О. С. Действие Уголовного кодекса России в отношении интернет-преступлений. М., 2013. С. 15.

² Фролов М. Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации: дис. ...канд. юрид. наук : 12.00.08. М., 2018. С. 123.

преступления. В основном, любые действия (ввод, модификация, блокирование, удаление) или вмешательство в функционирование средств хранения, обработки или передачи информации или информационно-телекоммуникационных сетей взаимозависимы от обстоятельств дела и могут включать как признаки приготовления к совершению компьютерного мошенничества, так и признаки покушения. Не всегда можно правильно и безусловно квалифицировать и разграничить приготовление и покушение на совершение мошенничества в сфере компьютерной информации.

Признак создания условий совершения преступления является главным при разграничении приготовления к преступлению от покушения. А. Ю. Решетников и Е. А. Русскевич в своей работе приводили пример приготовления к преступлению. По их мнению приготовлением может являться создание вредоносной программы или ее распространение через информационно-телекоммуникационную сеть в целях совершения преступления в дальнейшем, так же этом могут быть действия, направленные на создание сайтов-двойников или иных онлайн-ловушек, направленных на копирование персональной информации пользователей¹.

К тому же, действия, направленные на изъятие компьютерной информации, указывают на выполнение лицом объективной стороны преступления, предусмотренного ст. 159⁶ УК РФ. Если же деяние не было доведено до конца по независящим от виновного обстоятельствам (например, пресечение действий правоохранительными органами или работниками службы безопасности банка, сбой программы или оборудования и др.), в данном случае содеянное стоит квалифицировать как покушение на мошенничество в сфере компьютерной информации.

Так, например, в результате общения Л. с иным лицом, была достигнута договоренность о том, что иное лицо, содействуя Л. в реализации

¹ Решетников А. Ю., Русскевич Е. А. Некоторые вопросы квалификации неоконченных преступлений в сфере компьютерной информации. М., 2018. С. 88.

умысла на хищение чужого имущества, предоставит ему значимую информацию и средства совершения противоправного деяния, а именно: инструкцию по взлому банкомата, программное обеспечение для несанкционированного управления банкоматом, а так же коды доступа для автоматической выгрузки денежных средств из банкомата. Л., в свою очередь, во исполнение задуманного подыскал банкомат, подходящий по своим техническим характеристикам, приискал аккумуляторный шуруповерт и фрезу к нему для вскрытия корпуса банкомата и непосредственного доступа к ЭВМ (системному блоку). Также от иного лица получил вредоносную компьютерную программу, заведомо предназначенную для вмешательства в функционирование средств хранения, обработки, модификации компьютерной информации, нейтрализации средств защиты компьютерной информации и автоматической выгрузки денежных средств из банкомата в нарушение типового процесса выдачи наличных денежных средств банкоматом, а именно: после предъявления платежной карты, проверки корректности пин-кода карты, проверки наличия запрашиваемой к выдаче суммы на счету платежной карты. Реализуя задуманное, находясь в непосредственной близости от банкомата, Л. наблюдал за складывающейся обстановкой, выбирая удобное время для вскрытия корпуса банкомата. Однако, Л. не смог довести преступление до конца по не зависящим от него обстоятельствам, поскольку в процессе приготовления к совершению вышеуказанных противоправных действий был задержан сотрудником полиции. Л. Был признан виновным в совершении преступлений, предусмотренных ч. 2 ст. 273, ч. 1 ст. 30, ч. 3 ст. 159.6 УК РФ¹.

Покушением так же будет являться ситуация, когда преступник не смог распорядиться похищенным им имуществом потому как, например, по

¹ Приговор Октябрьского районного суда г. Владимира от 4 июня 2019 г. по делу № 1-95/2019.

независящим от него обстоятельствам банковский счет, который являлся объектом преступления, был заблокирован организацией.

Например, С., обладая навыками работы с ЭВМ и программным обеспечением, будучи осведомленным о порядке и принципах подключения к компьютерной сети «Интернет», имея корыстный преступный умысел, приобрел логин и пароль от аккаунта интернет-магазина «ozon.ru», владельцем которого являлся П., на пользовательском счете у которого находились денежные средства в сумме 11 500 рублей. Реализуя свой преступный умысел, С., осуществил неправомерный доступ к аккаунту потерпевшего и без его разрешения модифицировал персональные данные, изменив логин и пароль для доступа к аккаунту и получил доступ к компьютерной информации аккаунта потерпевшего и доступ к пользовательскому счету, заблокировав доступ для П. Продолжая свои преступные действия, С. сформировал заказ на приобретение товаров на общую сумму 11596 рублей, оплатив 11 500 рублей с пользовательского счета потерпевшего и 96 рублей 00 копеек через «Киви кошелек», принадлежащего С., указав свой адрес для доставки заказа, себя как получателя, а так же свой контактный мобильный телефон. Однако, указанный заказ был аннулирован сотрудниками интернет-магазина из-за подозрения в несанкционированном доступе, денежные средства возвращены на пользовательский счет П. и регистрационные данные восстановлены. Суд признал С. виновным в совершении преступлений, предусмотренных ч.2 ст. 272, ч.3 ст.30, ч.1 ст.159.6 УК РФ¹.

Так же, вопросом, вызывающим дискуссию в научной и практической среде является вопрос квалификации действий, как покушения на преступление, совершенное группой лиц, а именно момента приобретения

¹ Приговор Мотовилихинского районного суда г. Перми от 20 февраля 2019 г. по делу № 1-72/2019.

мошенником реальной возможности распорядиться похищенным имуществом, обусловленного действиями третьих лиц.

Согласно логике, данное хищение стоит считать оконченным с того момента, когда возможность по распоряжению имуществом появилась хотя бы у одного из соучастников. В соответствии с этим, можно сделать вывод, что если при распределении ролей похищенное имущество кладется на банковский счет одного из злоумышленников, а так же накапливается на нем, то в данных действиях соучастников как в таковых присутствует свидетельство об оконченном преступлении в отношении всех соучастников. И в обратном порядке, это подтверждает вывод, что существует покушение на мошенничество в сфере компьютерной информации, если отсутствует реальная возможность у конкретного лица распорядиться похищенным имуществом.

В свою очередь, вопрос о том, когда мошенничество в сфере компьютерной информации квалифицируется как единое продолжаемое преступление остается спорным как в науке, так и на практике.

Как правило, признаками продолжаемого преступления в сфере компьютерной информации представляются тождественность преступных действий, их совершение в короткий промежуток времени, а так же должен присутствовать единый умысел совершения преступлений в отношении всех потерпевших от проведенных мошеннических действий данным лицом. Однако есть случаи, когда мошенник не знает какое количество людей пострадает в результате его действий, например, когда способом совершения преступления является распространение вредоносного программного обеспечения, в результате загрузки которого происходит списание денежных средств потерпевшего¹. В результате проведения таких действий виновное лицо может не знать какой ущерб оно причинило, а так же какому

¹ Силаев С. А. Объективные признаки продолжаемого преступления. Кемерово, 2013. С. 280.

количеству людей, как было сказано ранее. Вместе с тем, очевидно, что множественность транзакций, совершенных данным путем, не может констатировать совокупность преступлений в данном случае¹.

Проблема соучастия в совершении компьютерного мошенничества также остается не до конца разрешенной и наиболее сложной при квалификации данного состава. При этом, в ситуациях, когда лицо обеспечивает свое физическое участие в совершении преступления или к подготовке к преступлению, предусмотренного ст. 159⁶ УК РФ (например, когда выполняет функцию организатора, пособника или подстрекателя), отсутствуют существенные отличия от соучастия в иных преступлениях. Однако, данное утверждение не может относиться к случаям, когда участие преступников организуется дистанционно. Согласно мнению А. Ю. Чупровой, особенностью подстрекательских действий с использованием информационно-телекоммуникационных сетей и, конечно, прежде всего сети "Интернет" является неперсонифицированный призыв к совершению преступления. Круг лиц, который может найти данное предложение, обратить на него внимание и одобрить его, принять участие в реализации, является неопределенным и большим².

Очень сложным представляется доказать именно факт подстрекательства в соучастии в данном преступлении, а не призыв к побуждению преступных действий или возбуждению интереса у лица к действиям, направленным против закона. Очевидно, что второй вариант не подстрекает лицо совершить конкретные действия в отношении чужого имущества. Подстрекательство включает в себя вложение определенных усилий, направленных на привлечение лиц, в том числе объяснение

¹ Фролов М. Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации: дис. ...канд. юрид. наук : 12.00.08. М., 2018. С. 130.

² Чупрова А. Ю. Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции: дис. ...д-ра. юрид. наук : 12.00.08. М., 2015. С. 258.

определенной выгода получаемой от преступления, преуменьшение значения последствий для потерпевшего, в том числе приложенных усилий и опасности, с которыми связано выполнение функций данного лица. А так же, способом привлечения других лиц в компьютерное мошенничество может являться угроза различного толка.

Согласно проведенным исследованиям М. Д. Фролова, почти половина опрошенных респондентов считают, то обстоятельство, что лицо не знает, кого именно ему удалось склонить к совершению мошенничества, путем подстрекательства с помощью сети "Интернет", и сколько таких лиц оказалось на само деле, не меняет характер и содержание его поведения¹.

Что же касается пособничества в сфере компьютерной информации, то данный вопрос вызывает аналогичную трудность для дачи правовой оценки преступления. Согласно доктрине, лицо признается пособником в совершении преступления, если оно совершало любое из действий, перечисленные в пункте 5 статьи 33 УК РФ (то есть подстрекателем признается лицо, которое помогает советами, указаниями, предоставлением информации, средств или орудий совершения преступления либо устранением препятствий, а также лицо, заранее обещавшее скрыть преступника, средства или орудия совершения преступления, следы преступления либо предметы, добывшие преступным путем, а равно лицо, заранее обещавшее приобрести или сбыть такие предметы²) и при этом было осведомлено об умысле всех участников преступления. Вместе с тем, непонятно как давать юридическую оценку действиям лица, которое с помощью сети "Интернет" распространяет информацию о способах совершения компьютерного мошенничества, дает возможность приобретения

¹ Фролов М. Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации: дис. ...канд. юрид. наук : 12.00.08. М., 2018. С. 131.

² Федеральный закон от 13.06.1996 № 63-ФЗ. Уголовный кодекс Российской Федерации.

специального оборудования и программного обеспечения, баз "слитых" персональных данных людей, в том числе отсканированных паспортов, "чистые" карты операторов сотовой связи и многое другое.

Согласно позиции А. Ю. Чупровой, действия такого лица и исполнителя в равной степени дополняют друг друга и являются составной частью общей деятельности по совершению мошенничества в сфере компьютерной информации. В пример приводит изготовителя отмычки и лица, которое совершило хищение из квартиры посредством отмычки. По ее мнению, разница заключается только в характере коммуникаций – в одном случае это виртуальный контакт, в другом – непосредственное общение¹.

Однако, с точки зрения теории уголовного права, если такое лицо понимает, что оно своими действиями способствует совершению преступления другими лицами, то содеянное не может образовать соучастия в форме пособничества.

С другой стороны, многие ученые, такие как А. Ю. Чупрова, М. Д. Фролов, А. А. Южин, С. А. Петров и др., считают что данный подход не может являться верным. Они исходят из того, что такое поведение лица является общественно опасным с объективной точки зрения, согласно их противоправному поведению они должны быть надлежащим образом квалифицированы и их действиям должна даваться надлежащая юридическая оценка.

Именно по этому предлагается игнорировать одностороннюю субъективную связь между лицами и признавать данные действия как соучастие в компьютерном мошенничестве². Ведь все таки лица склоняющие других на совершение компьютерного мошенничества или оказывающие

¹ Чупрова А. Ю. Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции: дис. ...д-ра. юрид. наук : 12.00.08. М., 2015. С. 261.

² Фролов М. Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации: дис. ...канд. юрид. наук : 12.00.08. М., 2018. С. 133.

содействие неограниченному кругу лиц в данном вопросе имеют абсолютно конкретные намерения, а не абстрактные. Именно потому что присутствует причинно-следственная связь стоит говорить о наличии признаков соучастия в данном составе преступления.

Однако, ученые подчеркивают, что устаревшие правовые конструкции выступают в качестве препятствия на пути борьбы с новыми разновидностями мошенничества. Они не являются мобильными и не способны подстраиваться под современные реалии, а ведь с каждым годом все чаще встречаются новые и более изощренные виды мошенничества.

Ведь если представить, что лицо совершило преступления, в нашем случае, благодаря полученной информации, "слитой" из кредитных организаций или различного вредоносного программного обеспечения, полученного от третьего лица, то без его участия преступник бы не смог получить данной информации самостоятельно. Соответственно, угроза наступления последствий не является абстрактной, а реальной. И конечно же, в связи с этим, есть основания утверждать о наличии в таких действиях преступного умысла и, как требуется, наличие признаков соучастия.

Так же, существуют ситуации, когда правоохранительные органы квалифицируют действия лица как мошенничество в сфере компьютерной информации, однако таковым вовсе не является.

Так, например, работником банка было зачислено на счет гражданину несколько сотен тысяч рублей, по невнимательности. Гражданин не растерялся и снял данную сумму со счета. В таком случае данные действия работника банка были не умышлены, в таких действиях нет состава компьютерного преступления, а наоборот, в действиях гражданина усматривается присвоение оказавшегося у него имущества. В этом случае действия гражданина должны квалифицироваться не как мошенничество в сфере компьютерной информации, а как неосновательное обогащение по гражданскому кодексу. В данной ситуации банк имеет обоснованное право подать гражданско-правовой иск об обязанности гражданина возвратить

неосновательное обогащение по статье 1102 ГК РФ. А так же направить иск о краже¹.

Кроме того, весомым вопросом в квалификации мошенничества в сфере компьютерной информации представляется ограничение его от смежных составов. Рассмотрение данного вопроса очень важно, чтобы понимать, какие признаки не характерны для мошенничества в сфере компьютерной информации. Так же, этот аспект вопроса очень важен, чтобы понимать отличие данного состава преступления от других, но об этом далее.

Подводя итог, стоит отметить, что:

- 1) местом совершения мошенничества в сфере компьютерной информации является территория, где совершено общественно опасное деяние, вне зависимости от того где наступили общественно опасные последствия;
- 2) приготовлением к преступлению могут быть любые действия, направленные на создание вредоносной программы, ее распространение через информационно-телекоммуникационную сеть в преступных целях, создание сайтов-двойников или иных онлайн-ловушек, направленных на копирование персональной информации пользователей и другие действия;
- 3) покушением на мошенничество в сфере компьютерной информации являются действия, направленные на выполнение лицом объективной стороны преступления, предусмотренного ст. 159⁶ УК РФ, и если же данные действия не были доведены до конца по независящим от виновного обстоятельствам, а так же, когда преступник не смог распорядиться похищенным им имуществом по независящим от него обстоятельствам;
- 4) в ситуациях, когда лицо обеспечивает свое физическое участие в совершении преступления или к его подготовке, предусмотренного статьей

¹ Апелляционное определение Верховного суда Чувашской Республики от 24.08.2017 по делу № 22-1995/2017

159⁶ УК РФ, отсутствуют существенные отличия от соучастия в иных преступлениях. Однако, когда имеет место дистанционное соучастие, стоит обращать внимание на то, что особенностью таких действий, как, например, подстрекательства производится посредством информационно-телекоммуникационных сетей, что значительно расширяет круг лиц, которые могут откликнуться на преступное предложение. Действия пособника в совершении мошенничества в сфере компьютерной информации предлагается не разграничивать с действиями исполнителя. Подстрекатели и пособники представляют реальную угрозу наступления последствий, однако, требуется наличие признаков соучастия.

2.2 Разграничение мошенничества в сфере компьютерной информации с иными составами преступлений

Первым делом стоит разграничить мошенничество в сфере компьютерной информации от кражи. Прежде всего, они отличаются способами совершения преступления. О том, какие действия квалифицируются как кража описано в п. 21 Постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 "О судебной практике по делам о мошенничестве, присвоении и растрате": "В тех случаях, когда хищение совершается путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным (тайно либо путем обмана воспользовался телефоном потерпевшего, подключенным к услуге «мобильный банк», авторизовался в системе интернет-платежей под известными ему данными другого лица и т.п.), такие действия подлежат квалификации как кража, если виновным не было оказано незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети. При этом изменение данных о состоянии банковского счета и (или) о движении денежных средств, произшедшее в результате использования виновным учетных данных потерпевшего, не может признаваться таким воздействием"¹.

Кроме того, Федеральным законом от 23.04.2018 № 111-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации" часть 3 статьи 158 УК РФ дополнена пунктом "Г", устанавливающим ответственность за хищение денежных средств с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159³ УК РФ). Квалификации по п. "Г" ч. 3 ст. 158 УК РФ также подлежат хищения денежных средств с банковских

¹ Постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 "О судебной практике по делам о мошенничестве, присвоении и растрате".

карт, совершенные путем использования вирусных программ. Например, на мобильный телефон потерпевшего поступает СМС-сообщение любого характера со ссылкой внутри него, после перехода по ссылке в телефон автоматически устанавливается вирусная программа, и преступник получает возможность проводить манипуляции со всем приложениями потерпевшего. В том числе с программами "Банк-Онлайн", в результате чего со счета потерпевшего похищаются денежные средства.

Если потерпевший не выполняет операцию по переводу денежных средств непосредственно со своего счета, а лишь сообщает преступнику все необходимые реквизиты, для выполнения операции, то в данном случае это стоит считать как обман, который направлен на облегчение доступа к чужому имуществу. В данном случае такие действия стоит квалифицировать как кража.

Мошенничество по ст. 159 УК РФ разграничивается от мошенничества в сфере компьютерной информации по ст. 159⁶ УК РФ главным образом тем, что при компьютерном мошенничестве имущество у потерпевшего изымается в результате его собственных (потерпевшего) действий и поведения, который был введен в заблуждение умышленными действиями виновного лица.

Таким же образом, похищенные персональные данные и их дальнейшее использование виновным лицом не является основанием для квалификации по ст. 159 УК РФ. Согласно решению суда, мошенничеством в сфере компьютерной информации будет являться то мошенничество, в результате которого гражданин Д. использовал достоверные персональные данные, а именно логин и пароль, для входа в систему "Мобильный банк". Суд посчитал, что действия, наплавленные на использование подлинных логинов и паролей для входа в систему не могут не служить основанием для привлечения лица в качестве обвиняемого по ст. 159⁶ УК РФ¹.

¹ Апелляционное решение суда г. Москвы от 06.05.2013 г. по делу №10-2076.

Так же, например, М. разместил заведомо ложное объявление о сдаче в аренду квартиру на сайте www.farpost.ru. Получал предоплату от потенциальных клиентов для исполнения определенных обязательств, однако их не выполнял и полученные денежные средства обращал в свою пользу. Предоплата вносилась потерпевшими добровольно на счет платежной системы «QIWI». Согласно приговору суда М. был признан виновным в совершении преступления, предусмотренного ч.1 ст. 159 УК РФ¹.

Согласно приговору Бийского городского суда от 13 октября 2020 г. по делу № 1-381/2020, С. был признан виновным в совершении преступления, предусмотренного п. "Г" ч. 3 ст. 159 УК РФ по следующим обстоятельствам: С., незаконно завладевший SIM-картой К., зная что к данной SIM -карте привязана функция мобильного банка и счета, открытого на имя К., посредством отправления СМС-сообщений о переводе денежных средств на номер 900 осуществил несколько переводов с банковской карты К. на свою дебетовую карту. В дальнейшем С. снял незаконно переведенные денежные средства со своей карты и распорядился ими по своему усмотрению².

Один из дискуссионных вопросов касается квалификации действий виновного лица при совершении хищения банковских денежных средств с предъявлением поддельного или чужого паспорта посредством автоматизированного процесса получения кредита (экспресс-кредита), без прямого контакта с кредитным менеджером. В данном случае стоит обратить внимание на предмет хищения – денежные средства, предоставляемые кредитной организацией согласно кредитному договору. Таким образом, исходя из предмета преступления, стоит сделать вывод, что данное деяние должно рассматриваться в рамках мошенничества в сфере кредитования по статье 159¹ УК РФ.

¹ Приговор Советского районного суда г. Владивостока от 29 июля 2020 г. по делу № 1-302/2020.

² Приговор Бийского городского суда от 13 октября 2020 г. по делу № 1-381/2020.

Так, например, В. умышленно, противоправно, из корыстных побуждений, введя в заблуждение администратора сайта ООО "И.", осуществляющего оформление кредита онлайн, относительно своих намерений, платежеспособности и возможности возвращения кредитных денежных средств, заранее зная, что выплачивать кредит не будет, посредствам сети "Интернет" предоставил подложные паспортные данные гражданина РФ на имя "О". Незаконно от имени "О" заключил с ООО "И." договор микрозайма и получив указанную сумму денежных средств В. распорядился ими по своему усмотрению, не предпринимая в дальнейшем каких-либо действий направленных на погашение займа, в результате чего причинил ООО "И." материальный ущерб. Согласно приговору суда, В. был признан виновным в совершении преступления, предусмотренного ч. 1 ст. 159¹ УК РФ¹.

Мошенничество с использованием электронных средств платежа по ст. 159³ УК РФ четко ограничивается от мошенничества в сфере компьютерной информации в п. 17 Постановления Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 " О судебной практике по делам о мошенничестве, присвоении и растрате": "действия лица следует квалифицировать по ст. 159³ УК РФ в случаях, когда хищение имущества осуществлялось с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем сообщения уполномоченному работнику кредитной, торговой или иной организации заведомо ложных сведений о принадлежности указанному лицу такой карты на законных основаниях либо путем умолчания о незаконном владении им платежной картой. В случаях когда лицо похитило безналичные денежные средства, воспользовавшись необходимой для получения доступа к ним конфиденциальной информацией держателя платежной карты (например, персональными данными владельца, данными платежной карты, контрольной

¹ Приговор Надымского городского суда от 5 июля 2019 г. по делу № 1-90/2019.

информацией, паролями), переданной злоумышленнику самим держателем платежной карты под воздействием обмана или злоупотребления доверием, действия виновного квалифицируются как кражи."¹.

То есть, в тех случаях, когда хищение осуществляется лицом с использованием поддельной или принадлежащей другому лицу любой расчетной картой и введением в заблуждение уполномоченного работника организации по поводу данных сведений, либо когда потерпевший под воздействием обмана самостоятельно переводит денежные средства на чужой расчетный счет (например, выполняя распоряжение злоумышленника, посредством операций через банкомат), осуществляется квалификация по ст. 159³ УК РФ. Так же, при оплате банковской картой "в одно касание" (то есть оплата, производимая посредством технологии бесконтактной оплаты и на сумму не более 1000 рублей, так как не требует введения ПИН-кода банковской карты) составляющая объективной стороны мошенничества в виде обмана либо злоупотребления доверием отсутствует. Таким образом, действия виновного образуют состав ст. 159³ УК РФ, поскольку имущество выбывает из ведения собственника тайно для него и помимо его воли.

Однако, некоторые ученые считают, что если хищение денежных средств осуществлялось без введения в заблуждение работника кредитной организации, вследствие работы с программным обеспечением, то деяние стоит квалифицировать по ст. 159⁶ УК РФ, так как содержит его признаки.

Согласно приговору Миасского городского суда Челябинской области К., находясь в гостях у знакомого и воспользовавшись тем, что он заснул, тайно завладел дебетовой картой. Далее, путем обмана работников торговой организации и умолчания о незаконном владении картой, произвел безналичный расчет с карты. Таким образом, причинил значительный вред потерпевшему. Был признан виновным в совершении преступления,

¹ Постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 "О судебной практике по делам о мошенничестве, присвоении и растрате".

предусмотренного ч. 2 ст. 159³ УК РФ, то есть мошенничества с использованием средств платежа с причинением значительного ущерба потерпевшему¹.

В данном случае обман не был направлен на завладение чужим имуществом (так как потерпевший спал в момент завладения картой), К. воспользовался дебетовой картой, принадлежащей другому лицу путем сообщения заведомо ложных сведений о принадлежности указанной карты К. на законных основаниях. Из приведенного примера понятно, что работник организации не осознает незаконность действий К., соответственно, не раскрывает обмана и не знает реального владельца. Согласно определению Судебной коллегии по уголовным делам ВС РФ от 29.09.2020 № 12-УДП20-5-К6, действующими нормативными актами на уполномоченных работников торговых организаций, осуществляющих платежные операции с банковскими картами, обязанность идентификации держателя карты по документам, удостоверяющим его личность, не возлагается².

Так же, например, А., используя вытекающие из служебных полномочий возможности для составления кредитного договора от имени клиентов ОАО "С" и получение в связи с этим денежных средств, принадлежащих ОАО "С.", воспользовавшись анкетными данными В., незаконно заполнила заявление на получение кредитной карты и сопутствующие документы, выполнив подписи от имени В., после чего незаконно получила кредитную карту с кредитным лимитом в сумме 60 000 рублей. После чего А. обналичила в банкомате ОАО "С." с кредитной карты, оформленной на имя В. денежные средства. Затем находясь в магазине А. воспользовалась кредитной картой, оформленной на В., и произвела оплату.

¹ Приговор Миасского городского суда от 30 декабря 2019 г. по делу № 1-765/2019.

² Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 29.09.2020 № 12-УДП20-5-К6

Суд признал А. виновной в совершении преступления, предусмотренного ч. 3 ст. 159³ УК РФ¹.

Так же, стоит рассмотреть вопрос разграничения состава мошенничества в сфере страхования по ст. 159⁵ УК РФ с компьютерным мошенничеством по ст. 159⁶ УК РФ. Согласно п. 8 Постановления Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 "О судебной практике по делам о мошенничестве, присвоении и растрате": "неправомерное завладение денежными средствами, иным чужим имуществом или приобретение права на него путем предъявления (представления) чужих личных или иных официальных документов (например, паспорта, пенсионного удостоверения, свидетельства о рождении ребенка) в зависимости от непосредственного объекта посягательства и иных обстоятельств дела квалифицируется как мошенничество соответственно по статьям 158¹, 159, 159¹, 159², 159³, 159⁵ УК РФ"². Ученые сходятся во мнении, что вне зависимости от того в какой форме были поданы документы (нарочно или электронно посредством сети "Интернет"), вне зависимости от того, контактировали ли вы с работником страховой организации или нет, деяние следует квалифицировать по ст. 159⁵ УК РФ. Однако, если решение о выплате осуществляется компьютерной программой автоматически, то данное деяние стоит оценивать как мошенничество в сфере компьютерной информации³.

Следующий вопрос по разграничению квалификации касается присвоения и растраты по ст. 160 УК РФ. Субъекты данного состава

¹ Приговор Октябрьского районного суда г. Новороссийска от 08.09.2015 по делу № 1-319/2015.

² Постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 "О судебной практике по делам о мошенничестве, присвоении и растрате".

³ Фролов М. Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации: дис. ...канд. юрид. наук : 12.00.08. М., 2018. С. 140.

преступления непосредственно связаны с осуществлением банковского обслуживания. Например, главный бухгалтер является лицом, начисляющим заработную плату работникам, рассчитывается по обязательствам с контрагентами и прочее, в настоящее время зачастую проводит платежи с помощью специализированных программ. Данный признак уже был рассмотрен ранее.

Например, Л., занимала должность главного бухгалтера образовательного учреждения. Согласно должностной инструкции, наделена организационно-распорядительными и административно-хозяйственными функциями, то есть обладает в указанном учреждении служебным положением. Л., обладая сведениями о том, что на расчетном счете образовательного учреждения находятся денежные средства, в том числе предназначенные для выплаты заработной платы сотрудникам образовательного учреждения, решила похитить вверенные ей денежных средства путем перечисления их на свой банковский счет под видом заработной платы в суммах заведомо больших, чем в действительности подлежало ей к выплате. С этой целью, находясь в рабочем кабинете подписывала своей электронно-цифровой подписью и направляла в банковские учреждения платежные поручения и реестры на выплату заработной платы, в которых была указана ее заработка плата в суммах заведомо больших, чем в действительности подлежало ей к выплате, тем сам противоправно безвозмездно обратила указанное вверенное ей имущество в свою пользу, Суд признал ее виновной в совершении преступления, предусмотренного ч. 3 ст. 160 УК РФ¹.

В сравнение мошенничества в сфере компьютерной информации (ст. 159⁶ УК РФ) и статьи 272 УК РФ – неправомерный доступ к компьютерной информации, можно сделать вывод, что в компьютерном мошенничестве

¹ Приговор Первомайского районного суда г. Кирова от 27 июля 2020 г. по делу № 1-225/2020.

указываются действия, которые должно осуществить виновное лицо (а именно ввод, удаление, блокирование, модификация или иное вмешательство), а в статье, посвященной неправомерному доступу к компьютерной информации – последствия, которые должны наступить (то есть уничтожение, блокирование, модификация и копирование) в результате незаконного доступа. Таким образом, когда наступят последствия указанной 272 статьи УК, в результате действий по ст. 159⁶ УК РФ, то согласно пункту 20 указанного Постановления Пленума Верховного Суда, требуется дополнительная квалификация. Соответствующая квалификация должна выполняться и при использовании для хищения имущества вредоносных компьютерных программ (ст. 273 УК РФ)¹.

Так же, в 2018 году появилась интересная практика. В 2015 году у А., обладавшего навыками работы с системой объединённых компьютерных сетей для хранения и передачи информации, действующего из корыстных побуждений, с целью получения постоянного источника дохода от занятия преступной деятельностью возник преступный умысел создать организованную группу, осуществляя активные действия по формированию организованной группы и вербовке лиц, склонных к совершению преступлений, вовлек по принципам знакомства и доверия К., Б., Д., с которыми поддерживал дружеские отношения, достоверно зная, что последние имеют в наличии переносные персональные компьютеры, а также навыки работы с сетью, предложив последним участвовать в организованной группе и совершать в ее составе. Они приняли предложение А., добровольно согласились на участие в организованной группе, а также на руководство А., рассчитывали на получение незаконной наживы от длительной преступной деятельности и были сплочены с А. одной целью – систематическим

¹ Бархатова Е. Н. Особенности квалификации мошенничества в сфере компьютерной информации и его разграничение с иными составами преступлений. Свирск, 2016. С. 115.

незаконным обогащением за счет совершения преступлений средней тяжести, тем самым, вступив в преступный сговор. Согласно договоренности, их группа занималась распространением в сети интернет ссылок на интернет-сайты, на которых размещены вредоносные компьютерные программы «вирусы», производили спам-рассылку СМС-сообщений неопределенному кругу лиц, содержащих ссылки на интернет-сайты, на которых размещены вредоносные компьютерные программы «вирусы», при переходе лиц по указанным ссылкам со смартфонов членам организованной группы становились известны данные об установленном на каждом конкретном мобильном устройстве граждан Российской Федерации приложении, а также получен доступ к СМС-сервису и приложению, позволяющему совершать переводы денежных средств со счетов банковских карт владельцев мобильных устройств, осуществляли переводы денежных средств со счетов банковских карт граждан Российской Федерации на счета банковских карт, счета электронных кошельков, мобильные счета SIM-карт, оформленных на неустановленных лица, проживающих в различных регионах РФ, неосведомленных об истинных намерениях участников организованной группы, посредством направления СМС-сообщений, специальных команд на сервисные номера банков Российской Федерации. Кроме этого, они блокировали доступ владельцев зараженных мобильных устройств к информации, находящейся на их мобильных устройствах, копировали информацию, содержащуюся в СМС-сообщениях с целью дальнейшего материального обогащения, и последующей в результате этого модификации информации, находящейся в сети ЭВМ банков Российской Федерации, осуществляли с помощью вредоносной программы «вирус» и веб-консоли (администрирующей панели) данного «вируса» переводы денежных средств со счетов банковских карт потерпевших.

Таким образом, суд признал их виновными в совершении преступлений, предусмотренных ч.2 ст .273, ч.3 ст . 272 , ч.3 ст .183, ч.4 ст . 159.6 УК РФ¹

При рассмотрении вопроса о разграничении квалификации преступления, предусмотренного ст. 327 УК РФ, то есть подделка, изготовление или оборот поддельных документов, государственных наград, штампов, печатей или бланков, и мошенничества в сфере компьютерной информации стоит опираться на позицию, указанную в п. 7 Постановления Пленума Верховного Суда РФ, где говорится, что данный состав стоит рассматривать как дополнение к ст. 159 УК РФ: "хищение лицом чужого имущества или приобретение права на него путем обмана или злоупотребления доверием, совершенные с использованием подделанного этим лицом официального документа, предоставляющего права или освобождающего от обязанностей, требует дополнительной квалификации по части 1 статьи 327 УК РФ", а так же " Хищение лицом чужого имущества или приобретение права на него путем обмана или злоупотребления доверием, совершенные с использованием изготовленного другим лицом поддельного официального документа, полностью охватывается составом мошенничества и не требует дополнительной квалификации по статье 327 УК РФ"². Но, как было сказано выше, мошенничество в сфере компьютерной информации характеризуется особым способом совершения преступления (не предполагает злоупотребление доверием потерпевшего или его обман), согласно этой особенности действия должны быть квалифицированы по совокупности преступлений.

¹ Приговор Центрального районного суда г. Читы от 23 октября 2018 г. по делу № 1-949/2018.

² Постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 "О судебной практике по делам о мошенничестве, присвоении и растрате".

Подводя итог, стоит отметить, что:

1) отличием мошенничества по ст. 159 УК РФ от преступления, предусмотренного ст. 159⁶ УК РФ, выступает то, что имущество у потерпевшего изымается в результате его собственных действий и поведения, потерпевший был введен в заблуждение умышленными действиями виновного лица;

2) предметом хищения по ст. 159¹ УК РФ являются денежные средства, предоставляемые кредитной организацией согласно кредитному договору. Таким образом, исходя из предмета преступления, стоит сделать вывод, что данное деяние должно рассматриваться в рамках мошенничества в сфере кредитования по статье 159¹ УК РФ, а не по ст. 159⁶ УК РФ, так как в данном случае виновное лицо никак не может воздействовать на работу информационно-телекоммуникационной сети или работу системы такого банка;

3) отличие мошенничества с использованием электронных средств платежа (ст. 159³ УК РФ) от мошенничества в сфере компьютерной информации (ст. 159⁶ УК РФ) заключается в том, что первый случай характеризуется обманом или злоупотреблением доверия в отношении человека (работника торговой организации, работника банка и т.д.), которому предоставляется не принадлежащая виновному лицу платежная карта или иное платежное средство (часы, телефон и др.);

4) говоря об отличии мошенничества в сфере страхования от компьютерного мошенничества, то вне зависимости от того в какой форме были поданы документы (нарочно или электронно посредством сети "Интернет"), вне зависимости от того, контактировали ли вы с работником страховой организации или нет, деяние следует квалифицировать по ст. 159⁵ УК РФ. Однако, если решение о выплате осуществляется компьютерной программой автоматически или имело место вмешательство в работу системы, то данное деяние стоит оценивать как мошенничество в сфере компьютерной информации;

5) при отличии мошенничество в сфере компьютерной информации от присвоения и растраты (ст. 160 УК РФ) следует иметь ввиду, что во втором случае на момент изъятия имущества предмет хищения является вверенным виновному лицу;

6) в сравнении мошенничества в сфере компьютерной информации (ст. 159⁶ УК РФ) и статьи 272 УК РФ – неправомерный доступ к компьютерной информации, можно сделать вывод, что в компьютерном мошенничестве указываются действия, которые должно осуществить виновное лицо (а именно ввод, удаление, блокирование, модификация или иное вмешательство), а в статье, посвященной неправомерному доступу к компьютерной информации – последствия, которые должны наступить (то есть уничтожение, блокирование, модификация и копирование) в результате незаконного доступа. Таким образом, когда наступят последствия указанной 272 статьи УК, в результате действий по ст. 159⁶ УК РФ, то требуется дополнительная квалификация (по ст. 272 или ст. 273 УК РФ).

ЗАКЛЮЧЕНИЕ

В заключительной части исследования стоит сделать следующие выводы.

Мошенничество в сфере компьютерной информации имеет такой непосредственный объект, как охраняемые законом отношения в сфере собственности. Дополнительный, факультативный объект – охраняемые законом общественные отношения, касающиеся информационной безопасности.

Предметом мошенничества в сфере компьютерной информации выступает имущество и право на имущество – электронные, безналичные деньги, бездокументарные ценные бумаги, цифровые финансовые активы, виртуальные объекты имущества (приобретаемое за реальные деньги и обладающее финансовой ценностью), а так же персональная информация потерпевшего и другое.

Способами совершения мошенничества в сфере компьютерной информации являются действия, связанные с вводом, удалением, блокированием, модификацией компьютерной информации, а так же вмешательство в функционирование средств хранения, обработки, передачи компьютерной информации, а так же вмешательство в функционирование информационно-телекоммуникационных сетей. К тому же, к способам совершения мошенничества в сфере компьютерной информации может относиться обман или злоупотребление доверием, однако, данный признак не является характерным, как правило, данное преступление не предусматривает наличие контакта между лицом, совершающим мошеннические действия с потерпевшим лицом. Данные действия совершаются для воздействия на компьютерную информацию, а обман или злоупотребление доверием, в исключительных случаях, служат способами достижения получения доступа к компьютеру и информационной системе.

Мошенничество в сфере компьютерной информации по конструкции является материальным составом. Считается оконченным с момента, когда имущество поступило в незаконное владение лица и когда оно получило реальную возможность распоряжаться и пользоваться по своему усмотрению данным имуществом. Местом совершения мошенничества в сфере компьютерной информации является территория, где совершено общественно опасное деяние, вне зависимости от того где наступили общественно опасные последствия.

Субъектом мошенничества в сфере компьютерной информации является вменяемое физическое лицо, достигшее шестнадцатилетнего возраста на момент совершения деяния. Совершая преступление лицо осознает общественную опасность, предвидит неизбежность наступления последствий и желает их наступления. Соответственно, субъективная сторона мошенничества в сфере компьютерной информации характеризуется умышленной формой вины с прямым умыслом. Виновный преследует корыстную цель, вне зависимости от его мотива.

Такой признак как значительный ущерб носит оценочный характер, минимальный размер которого установлен в ст. 7.27 КоАП РФ и составляет не более 2500 рублей, а максимальный размер ущерба не должен превышать 250 тысяч рублей. Крупный размер не должен превышать миллиона рублей, а особо крупный превышает миллион рублей;

Групповой характер совершения мошенничества в сфере компьютерной информации может заключаться в осуществлении соисполнителями разных функций или способов совершения преступления, например, одним соисполнителем – блокирование информации на компьютере, а другим может заключаться в любом ином вмешательстве в функционировании информационно-телекоммуникационной сети.

Признак организованной группы в ч. 4 ст. 159⁶ УК РФ вступает в силу, если указанные действия совершены устойчивой группой лиц, которые

заранее объединились и подготовились к совершению одного или нескольких преступлений.

Приготовлением к преступлению могут быть любые действия, направленные на создание вредоносной программы, ее распространение через информационно-телекоммуникационную сеть в преступных целях, создание сайтов-двойников или иных онлайн-ловушек, направленных на копирование персональной информации пользователей и другие действия;

Покушением на мошенничество в сфере компьютерной информации являются действия, направленные на выполнение лицом объективной стороны преступления, предусмотренного ст. 159⁶ УК РФ, и если же данные деяния не были доведены до конца по независящим от виновного обстоятельствам, а так же, когда преступник не смог распорядиться похищенным им имуществом по независящим от него обстоятельствам.

В ситуациях, когда лицо обеспечивает свое физическое участие в совершении преступления или к его подготовке, предусмотренного статьей 159⁶ УК РФ, отсутствуют существенные отличия от соучастия в иных преступлениях. Однако, когда имеет место дистанционное соучастие, стоит обращать внимание на то, что особенностью таких действий, как, например, подстрекательства производится посредством информационно-телекоммуникационных сетей, что значительно расширяет круг лиц, которые могут откликнуться на преступное предложение. Действия пособника в совершении мошенничества в сфере компьютерной информации предлагается не разграничивать с действиями исполнителя. Подстрекатели и пособники представляют реальную угрозу наступления последствий, однако, требуется доказанное наличие признаков соучастия.

Такой признак, как совершение преступления лицом с использованием своего служебного положения имеет отношение к лицам, приведенным в примечании к ст. 285 УК РФ и ст. 201 УК РФ.

Отличием мошенничества по ст. 159 УК РФ от преступления, предусмотренного ст. 159⁶ УК РФ, выступает то, что имущество у

потерпевшего изымается в результате его собственных действий и поведения, потерпевший был введен в заблуждение умышленными действиями виновного лица;

Предметом хищения по ст. 159¹ УК РФ являются денежные средства, предоставляемые кредитной организацией согласно кредитному договору. Таким образом, исходя из предмета преступления, стоит сделать вывод, что данное деяние должно ограничиваться от ст. 159⁶ УК РФ и рассматриваться в рамках мошенничества в сфере кредитования по статье 159¹ УК РФ, так как в данном случае виновное лицо никак не может воздействовать на работу информационно-телекоммуникационной сети или работу системы такого банка.

Отличие мошенничества с использованием электронных средств платежа (ст. 159³ УК РФ) от мошенничества в сфере компьютерной информации (ст. 159⁶ УК РФ) заключается в том, что первый случай характеризуется обманом или злоупотреблением доверия в отношении человека (работника торговой организации, работника банка и т.д.), которому предоставляется не принадлежащая виновному лицу платежная карта или иное платежное средство (часы, телефон и др.).

Говоря об отличии мошенничества в сфере страхования от компьютерного мошенничества, то вне зависимости от того в какой форме были поданы документы (нáрочно или электронно посредством сети "Интернет"), вне зависимости от того, контактировали ли вы с работником страховой организации или нет, деяние следует квалифицировать по ст. 159⁵ УК РФ. Однако, если решение о выплате осуществляется компьютерной программой автоматически или имело место вмешательство в работу системы, то данное деяние стоит оценивать как мошенничество в сфере компьютерной информации.

При отличии мошенничество в сфере компьютерной информации от присвоения и растраты (ст. 160 УК РФ) следует иметь ввиду, что во втором

случае на момент изъятия имущества предмет хищения является вверенным виновному лицу.

В сравнении мошенничества в сфере компьютерной информации (ст. 159⁶ УК РФ) и статьи 272 УК РФ – неправомерный доступ к компьютерной информации, можно сделать вывод, что в компьютерном мошенничестве указываются действия, которые должно осуществить виновное лицо (а именно ввод, удаление, блокирование, модификация или иное вмешательство), а в статье, посвященной неправомерному доступу к компьютерной информации – последствия, которые должны наступить (то есть уничтожение, блокирование, модификация и копирование) в результате незаконного доступа. Таким образом, когда наступят последствия указанной 272 статьи УК, в результате действий по ст. 159⁶ УК РФ, то требуется дополнительная квалификация (по ст. 272 УК РФ).

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативные правовые акты

1. О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий [Электронный ресурс] : Постановление Пленума Верховного Суда Российской Федерации от 16 октября 2009 г. № 19 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

2. О судебной практике по делам о краже, грабеже и разбое[Электронный ресурс] : Постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2002 г. № 29 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

3. О судебной практике по делам о мошенничестве, присвоении и растрате [Электронный ресурс] : Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

4. Об информации, информационных технологиях и о защите информации [Электронный ресурс] : федер. закон от 27.07.2006 N 149-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

5. Соглашение "О сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации [Электронный ресурс] : федер. закон от 01.10.2008 № 164-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

6. Уголовный кодекс Российской Федерации [Электронный ресурс] : федер. закон от 13.06.1996 № 63-ФЗ ред. от 24.02.2021. // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

Материалы судебно-следственной практики

7. Апелляционное определение Верховного суда Чувашской Республики от 24.08.2017 по делу № 22-1995/2017 [Электронный ресурс]. // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

8. Апелляционное постановление Верховного Суда Республики Саха (Якутия) от 26 октября 2017 г. по делу № 22К-1671/2017 [Электронный ресурс]. // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

9. Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 29.09.2020 № 12-УДП20-5-К6 [Электронный ресурс]. // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

10. Постановление Советского районного суда г. Красноярска от 18 июня 2019 г. по делу № 1-675/2019 [Электронный ресурс]. // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

11. Приговор Бийского городского суда от 13 октября 2020 г. по делу № 1-381/2020 [Электронный ресурс]. // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

12. Приговор Замоскворецкого районного суда г. Москвы от 6 февраля 2015 г. по делу № 1-52/2015 [Электронный ресурс]. // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

13. Приговор Каспийского городского суда от 26 июня 2013 года по делу № 1-130/2013 [Электронный ресурс]. // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

14. Приговор Миасского городского суда от 30 декабря 2019 г. по делу № 1-765/2019 [Электронный ресурс]. // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

15. Приговор Мотовилихинского районного суда г. Перми от 20 февраля 2019 г. по делу № 1-72/2019 [Электронный ресурс]. // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

16. Приговор Надымского городского суда от 5 июля 2019 г. по делу № 1-90/2019 [Электронный ресурс]. // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

17. Приговор Октябрьского районного суда г. Владимира от 4 июня 2019 г. по делу № 1-95/2019 [Электронный ресурс]. // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

18. Приговор Октябрьского районного суда г. Новороссийска от 08.09.2015 по делу № 1-319/2015 [Электронный ресурс]. // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

19. Приговор Первомайского районного суда г. Кирова от 27 июля 2020 г. по делу № 1-225/2020 [Электронный ресурс]. // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

20. Приговор Промышленного районного суда г. Самара Самарской области от 4 октября 2016 г. по делу № 1-206/2016 [Электронный ресурс]. // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

21. Приговор Симоновского районного суда г. Москвы от 14 февраля 2013 г. по делу № 1-79/2013 [Электронный ресурс]. // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

22. Приговор Советского районного суда г. Владивостока от 29 июля 2020 г. по делу № 1-302/2020 [Электронный ресурс]. // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

23. Приговор Фрунзенского районного суда г. Саратова от 19 июля 2018 г. по делу № 1-66/2018 [Электронный ресурс]. // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

24. Приговор Хорошевского районного суда г. Москвы от 28 ноября 2014 г. по делу № 1-585/2014 [Электронный ресурс]. // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

25. Приговор Центрального районного суда г. Читы от 23 октября 2018 г. по делу № 1-949/2018 [Электронный ресурс]. // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

Научные источники

26. Бархатова, Е. Н. Особенности квалификации мошенничества в сфере компьютерной информации и его разграничение с иными составами преступлений / Е. Н. Бархатова // Современное право. – 2016. – № 9. – С. 110–115.

27. Безверхов, А. Г. Мошенничество и его виды: вопросы законодательной регламентации и квалификации / А. Г. Безверхов // Уголовное право. – 2015. – № 5. – С. 8–14.

28. Беляев, Н. А. Курс советского уголовного права. Часть общая / под ред. Н. А. Беляева, М. Д. Шаргородского. – Ленинград: Издательство Ленинградского университета, 1968. – 648 с.

29. Бриллиантов, А. В. Комментарий к Уголовному кодексу Российской Федерации: В 2 т. Т. 2 (постатейный) [Электронный ресурс] / под ред. А. В. Бриллиантова // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

30. Гладких, В. И. Уголовное право России. Общая и Особенная части. / под ред. В. И. Гладких, В. С. Курчева. – М.: Новосибирский государственный университет, 2015. – 634 с.

31. Гузеева, О. С. Действие Уголовного кодекса России в отношении интернет-преступлений / О. С. Гузеева // Законы России: опыт, анализ, практика. – 2013. – № 10 — С. 15–19.

32. Егорова, Н. А. Ответственность за служебные мошенничества: необходимость нового подхода / Н. А. Егорова // Российская юстиция. – 2014. – № 8. – С. 19–22.

33. Еремеева, А. Д. К вопросу о способах совершения мошенничества в сфере компьютерной информации / А. Д. Еремеева // Вестник студенческого научного общества ГОУ ВПО "Донецкий национальный университет". – 2020. – № 12–1. – С. 154–157.

34. Журавлева, Г. В. Мошенничество в сфере компьютерной информации: спорные вопросы теории и практики / Г. В. Журавлева, Н. А. Карпова // Вестник Московского университета МВД России. – 2017. – № 5. – С. 153–158.

35. Игнатов, А. Н. Уголовное право России. Учебник для вузов. В 2-х томах. Т. 1. Общая часть / под ред. А. Н. Игнатова, Ю. А. Красикова. – М.: Издательство НОРМА, 2000. – 639 с.

36. Капинус, О. С. Уголовное право России. Общая часть : учебник для бакалавриата, специалитета и магистратуры / О. С. Капинус. – М.: Издательство Юрайт, 2019. – 704 с.

37. Карапович, М. К. Квалификация преступлений: понятие, особенности и проблемы / М. К. Карапович // Законность и правопорядок в современном обществе. – 2014. – № 22 – С. 161–166.

38. Кибальник, А. Г. Квалификация мошенничества в новом Постановлении Пленума Верховного Суда РФ / А. Г. Кибальник // Уголовное право. – 2018. – № 1. С. 61–67.

39. Коновалова, Е. В. Особенности объекта и предмета преступления, предусмотренного ст. 159⁶ УК РФ / Е. В. Коновалова // Цифровые технологии в юриспруденции: генезис и перспективы. – 2020. – С. 65–67.

40. Кулешова, Н. Н. Особенности квалификации мошенничества в сфере компьютерной информации / Н. Н. Кулешова, Е. И. Христофорова // Вестник Алтайской академии экономики и права. – 2019. – № 6. – С. 105–109.

41. Кулешова, Н. Н. Особенности квалификации мошенничества в сфере компьютерной информации / Н. Н. Кулешова, Е. И. Христофорова // Вопросы науки и образования. – 2018. – № 14 (26). – С. 41–46.
42. Лебедев В. М. Комментарий к Уголовному кодексу Российской Федерации [Электронный ресурс] / под ред. д. ю. н., председателя Верховного Суда РФ В. М. Лебедева // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.
43. Лихолетов, А. А. Проблемы разграничения мошенничества с использованием платежных карт с другими составами преступлений / А. А. Лихолетов // Российская юстиция. – 2017. – № 6. – С. 35–37.
44. Лопатина, Т. М. Проблемы уголовно-правовой защиты сферы компьютерной информации: современный взгляд на мошенничество / Т. М. Лопатина // Право и безопасность. – 2013. – № 3 – 4 (45). – С. 89–95.
45. Медведев, С. С. Мошенничество в сфере высоких технологий: автореф. дис. ...канд. юрид. Наук : 12.00.08 / Медведев Сергей Сергеевич. – Краснодар, 2008. – 22 с.
46. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации утв. Генеральной прокуратурой РФ 30.05.2014 [Электронный ресурс]. Режим доступа: URL: <https://genproc.gov.ru>.
47. Петров, С. А. Хищение чужого имущества или приобретение права на него путем обмана: уголовно-правовая оценка и совершенствование правовой регламентации : автореф. дис. ...канд. юрид. Наук : 12.00.08 / Петров Станислав Анатольевич. – Москва, 2015. – 31 с.
48. Плотников, А. И. Уголовное право России. Общая часть: учебник / А. И. Плотников. – Оренбург: ООО ИПК «Университет», 2016. – 443 с.
49. Побегайло, А. Э. Киберпреступность: учебное пособие для бакалавров. / А. Э. Побегайло. – Москва: Ун-т прокуратуры Российской Федерации, 2014. –184 с.

50. Подвойкина, И. А. Уголовное право в 2 т. Т. 1. Общая часть : учебник для бакалавров / отв. ред. И. А. Подвойкина, Е. В. Серегина, С. И. Улезько. — Москва: Издательство Юрайт, 2014. — 590 с.

51. Прозументов, Л. М. Организованная группа как форма соучастия в преступлении в действующем российском законодательстве / Л. М. Прозументов // Вестник Томского государственного университета. Право. – 2015. – № 4 (18) – С. 60–69.

52. Рарог, А. И. Проблемы квалификации преступлений по субъективным признакам: монография / А. И. Рарог. – Москва: Проспект, 2015. – 232 с.

53. Ревин, В. П. Уголовное право России. Общая часть / под ред. В. П. Ревина. – М.: Юстицинформ, 2016. –580 с.

54. Решетников, А. Ю. Некоторые вопросы квалификации неоконченных преступлений в сфере компьютерной информации / А. Ю. Решетников, Е. А. Русскевич // Уголовное право. – 2018. – № 2 – С. 86–95.

55. Русскевич, Е. А. Новое постановление Пленума Верховного Суда Российской Федерации о квалификации мошенничества в сфере компьютерной информации / Е. А. Русскевич // Уголовный процесс – 2018. – № 2 – С. 63–69.

56. Русскевич, Е. А. Новые нормы УК РФ об электронном мошенничестве и коррупционных преступлениях / Е. А. Русскевич // Уголовный процесс. – 2018. – № 7 – С. 26–32.

57. Силаев, С. А. Объективные признаки продолжаемого преступления / С. А. Силаев // Вестник Кемеровского государственного университета. – 2013. – № 3–1 (55). – С. 278–283.

58. Фролов, М. Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации: дис. ...канд. юрид. Наук : 12.00.08 / Фролов Михаил Дмитриевич. – Москва, 2018. – 211 с.

59. Хилюта, В. В. Хищение с использованием компьютерной техники или компьютерное мошенничество? / В. В. Хилюта // Библиотека криминалиста. – 2013. – № 2 (24). – С. 55–65.

60. Чупрова, А. Ю. Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции: дис. ...д-ра. юрид. наук : 12.00.08 / Чупрова Антонина Юрьевна. – Москва, 2015. – 608 с.

61. Шеслер, А. В. Содержание умысла по действующему российскому уголовному законодательству / Шеслер А. В. // Вестник Владимира юридического института. – 2017. – № 3 (44). – С. 135–138.

62. Энгельгардт, А. А. Вопросы квалификации мошенничества в сфере компьютерной информации / А. А. Энгельгардт // Право. Журнал высшей школы экономики – 2016. – № 4. – С. 86 – 95.

63. Южин, А. А. Мошенничество и его виды в российском уголовном праве: автореф. дис. ...канд. юрид. Наук : 12.00.08 / Южин Андрей Андреевич. – Москва, 2016. – 22 с.

Иные источники

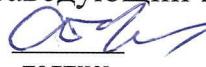
64. Официальный сайт Судебного Департамента при Верховном Суде Российской Федерации [Электронный ресурс]. Режим доступа: URL: <http://www.cdep.ru>.

65. Официальный сайт Генеральной прокуратуры Российской Федерации [Электронный ресурс]. Режим доступа: URL: <https://genproc.gov.ru>.

66. Официальный сайт Министерства внутренних дел Российской Федерации [Электронный ресурс]. Режим доступа: URL: <https://mvd.ru>.

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Юридический институт
Кафедра уголовного права

УТВЕРЖДАЮ
Заведующий кафедрой
 А. Н. Тарбагаев
подпись инициалы, фамилия
« 21 » 06 2021г.

БАКАЛАВРСКАЯ РАБОТА

40.03.01 – Юриспруденция

Проблемы квалификации
мошенничества в сфере компьютерной информации
(ст. 159⁶ УК РФ)

Руководитель П. Л. Сурихин
доцент, канд. юрид. наук
подпись, дата 26.05.2021
должность, учёная степень инициалы, фамилия

Выпускник К. К. Чупыра
Чуп 25.05.2021
подпись, дата инициалы, фамилия

Красноярск 2021