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

Юридический
институт
Уголовного права
кафедра

УТВЕРЖДАЮ

Заведующий кафедрой

_____ А.Н. Тарбагаев
подпись

« ___ » _____ 2021 г.

# БАКАЛАВРСКАЯ РАБОТА

40.03.01 - Юриспруденция
код – наименование направления

Уголовно-правовая характеристика преступления, предусмотренного ч.1 ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации»

тема

Руководитель _____ к.ю.н., доцент С.И. Бушмин
подпись, дата должность, ученая степень инициалы, фамилия

Выпускник _____ Р.Р. Дубинникова
подпись, дата инициалы, фамилия

Красноярск 2021

**Содержание**

# Введение

В связи с переходом к информационному обществу и всемирной глобализации всех процессов, а также внедрением высоких технологий в повседневную жизнь человека, наблюдаются существенные изменения в различных сферах жизнедеятельности, а именно расширяются возможности оказания воздействия на личность и собственность. Соответственно, на современном этапе развития отношений государства и личности, перед законодателем появляется необходимость регулирования и законодательно-нормативной регламентации процессов в сфере информационных технологий.

Несмотря на положительное воздействие высоких технологий на общество и государство, а именно ускорение процессов коммуникации, упрощенный доступ к информационным ресурсам, внедрение процессов цифровизации для повышения качества и развития экономики и т.д. процесс информатизации несет в себе ряд негативных последствий. Так, в настоящее время стихийно появляются новые формы и виды преступных посягательств. Специфика преступлений в сфере компьютерной информации предполагает достаточно высокую возможность сокрытия содеянного, сложность выявления и разграничения составов. Также данные преступления обладают особенностями расследования, поиском доказательной базы и интеллектуальным характером преступной деятельности.

Учитывая специфику информационного пространства со стороны преступников разрабатываются все более изощренные способы получения имущественной выгоды. Так, в 2012 году законодатель закрепил в УК РФ ответственность за  новый состав преступления, а именно мошенничество в сфере компьютерной информации.

Актуальность данного исследования обусловлена тем, что судебная практика сталкивается с различными сложностями при квалификации и отграничении данного вида преступлений от смежных составов. Это

подтверждается различием вынесенных приговоров судами первой, апелляционной и кассационной инстанциями, а также противоречиями этих решений с доктринальными позициями ряда ученых.

В связи с вышеизложенным тема настоящего исследования является актуальной в научном и практичном плане.

Целью настоящего исследования является выявление дискуссионных вопросов и предложений по совершенствованию законодательства.

Из поставленной цели вытекают следующие задачи:

- провести исследование понятия мошенничества в сфере компьютерной информации;

- провести анализ международно-правовых актов об уголовной ответственности за компьютерное мошенничество;

- раскрыть и охарактеризовать объективные и субъективные признаки состава преступления.

- провести сравнительный анализ преступления, предусмотренного ст.159.6 УК РФ от смежных составов.

Объектом исследования являются уголовно-правовые отношения, складывающиеся по поводу толкования и применения нормы, предусмотренной ст. 159.6 УК РФ.

Предметом исследования являются международно-правовые акты; нормы Российского уголовного законодательства; судебная практика; научная и учебная литература о мошенничестве в сфере компьютерной информации.

Теоретической основой исследования являются труды таких ученых как:

А.В. Бриллиантов, В.К. Барчуков, Т.А. Бушуев, М.Ю. Дворецкий, А.В. Наумов, Г.П. Новоселов и др.

Работа состоит из введения, трех глав и заключения.

Эмпирической базой исследования являлась опубликованная практика рассмотрения уголовных дел судами Республики Башкортостан, Брянской

области, Белгородской области, Владимирской области, Курской области, Ульяновской области, за период с 2013 по 2021 год.

# Глава 1. Уголовное законодательство зарубежных стран об ответственности за мошенничество в сфере компьютерной информации

## 1.1 Уголовное законодательство Европы и Соединенных Штатов Америки

За последнее время, преступления с сфере компьютерной информации распространились по всему миру и достигли глобальных масштабов. При постоянном развитии информационных технологий, изменяются и виды преступлений. Следовательно, мировое сообщество, оценивая данную ситуацию, постоянно находится решения проблемы противостояния киберпреступлениям. Оно собирает информацию, исследует ее, анализирует, и предлагает выработку ответных мер по противодействию такого рода преступлениям на мировом уровне. Также, можно сделать вывод о том, что необходимо постоянное и своевременное совершенствование законодательства в сфере компьютерной информации и технологий. Рассмотрим более подробно состав мошенничества в сфере компьютерной информации на примере романо-германской и англо-саксонской правовой семьи, а именно его состав и особенности квалификации.

В первую очередь, обратимся к романо-германской правовой семье. Из курса теории государства и права, нам известно, что к романо-германской правовой семье относятся правовые системы государств континентальной Европы. У данной правовой семьи имеется ряд особенностей. Так, в качестве основного источника права государств романо-германской правовой семьи является нормативный акт. Структура права характеризуется делением на частное и публичное, суды лишены возможности заниматься законодательной и правотворческой деятельностью.[1]

[1] Саидов А.Х. Сравнительное правоведение (основные правовые системы современности): учебник / под ред. В.А. Туманова. М.: «Юристъ», 2003. С. 144.

Все вышеперечисленные особенности применимы также и к уголовному законодательству, в которое включается киберпреступность, а именно рассматриваемый нами состав мошенничества с использованием компьютерных технологий. Согласно ст.8 Конвенции о преступности в сфере компьютерной информации №185, которая была ратифицирована не только странами Совета Европы, государства должны принять необходимые меры для того, чтобы квалифицировать в качестве уголовных преступлений, в случае совершения умышленно и неправомерно, лишения другого лица его собственности путем любого ввода, изменения, удаления или блокирования компьютерных данных либо любого вмешательства в функционирование компьютерной системы, мошенническим или бесчестным намерением неправомерного извлечения экономической выгоды для себя или для иного лиц.[2]

Противодействие схожим преступлениям имеет принципиальное значение во всех, рассмотренных нами государствах. Невзирая на некоторые различия в позиции законодателей мошенничество в сфере компьютерной информации совершается с использованием информационных технологий определяется как посягательство на собственность. Защита от подобного рода посягательств является одной из основных функций любого государства.

Одной из первых стран, включивших в свой Уголовный кодекс ответственность за преступления с использованием компьютерной информации было Королевство Швеция. Сам Уголовный кодекс был принят в 1962 г., вступил в силу в 1965 г.. В кодексе отсутствует отдельная статья о компьютерном мошенничестве, данный вид преступного деяния является составной частью нормы о мошенничестве. В ч. 1 ст. 1 главы 9 «О мошенничестве и Обмане» УК Швеции определяется простой состав

[2] Конвенция о преступности в сфере компьютерной информации (ETS No 185) [рус., англ. ] ( Заключена в г. Будапеште 23.11.2001) (с изм. от 28.01.2003) [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

мошенничества.[3] А вот в ч.2 ст.1 главы 9 УК Швеции закреплено, что также должно быть приговорено за мошенничество лицо, которое путем предоставления неправильной и неполной информации, или внесения изменений в программу или отчетность, или каким-либо другим способом незаконно влияет на результат автоматической обработки информации или любой другой сходной автоматической обработки, которая влечет выгоду для лица, совершившего преступление и убытки для любого другого лица.

Объективная сторона данного вида преступления состоит в одном из нескольких действий - предоставлении неправильной или неполной информации, внесении изменений в программу либо каким-либо другим способом незаконно влиять на результат обработки информации. Состав, практически как и во всех европейских странах является материальным, так как выгода, полученная одним лицом, обязательно должна нести убытки второму лицу. Между деянием и последствием необходимо наличие причинно-следственной связи.

Санкция нормы за компьютерное мошенничество предусматривается такая же, как и за простое мошенничество. Согласно ст.3 главы 9 УК Швеции, наиболее строгим наказанием за совершенное мошенничество с отягчающими обстоятельствами является лишение свободы на срок от шести месяцев до шести лет.

Подобным образом мошенничество в сфере компьютерной информации определяется уголовными кодексами других стран Скандинавского полуострова. Например, в Уголовном кодексе Финляндии статья о компьютерном мошенничестве содержится в главе 36 с аналогичным, как в Швеции названием «О мошенничестве и обмане»[4]. В то же время, вопреки шведскому уголовному законодательству, Уголовный кодекс Финляндии содержит более подробную систему отягчающих

[3] Уголовный кодекс Швеции [Электронный ресурс] // – Режим доступа: http://www.loc.gov/law/help/guide/nations/sweden.php.

[4] Уголовный кодекс Финляндии. [Электронный ресурс] // – Режим доступа: http://legislationline.org/documents/section/criminal-codes.

обстоятельств, например если деяние совершено с использованием своего доверительного положения; если был нанесен значительный ущерб; если деяние совершено в отношении лица, находящегося в иждивенческом положении и т.д. Данные квалифицирующие признаки наказывается лишением свободы на срок от 4 месяцев до 4 лет.

В Германии, согласно Уголовному кодексу, принятому в мае 1871г., компьютерное мошенничество входит в раздел «Преступления против собственности».[5] А именно в главу 22 под названием «Мошенничество и преступное злоупотребление доверием», который включает в себя десять параграфов. Согласно статье 263а тот, кто умышленно или с намерением создать для себя или третьего лица противоправную имущественную выгоду наносит ущерб другому лицу тем, что влияет на результат обработки данных, создавая неправильные программы, используя неправильные или неполные данные, неправомочно используя данные или иным образом неправомерно воздействуя на указанный процесс, наказывается лишением свободы на срок до пяти лет или денежным штрафом. По справедливому мнению А.В. Серебренниковой, выделение данного состава из общей нормы, предусматривающей уголовную ответственность за мошенничество, направлено на то, чтобы компенсировать отсутствие в УК ФРГ раздела о преступных деяниях в сфере компьютерной информации.[6]

Объектом этого преступления являются отношения собственности. Предметом посягательства является имущество лица. Под имуществом лица в целом в германской уголовно-правовой доктрине понимается вся совокупность экономических благ потерпевшего, включая вещи, права требования и иные объекты гражданских прав. Следовательно норма о компьютерном мошенничестве охраняет все экономические блага лица, включая как вещи, так и иные объекты гражданских прав.

---

[5] Уголовный кодекс Германии [Электронный ресурс] // – Режим доступа: http://www.gesetze-im-internet.de/englisch_stgb/ englisch_stgb. html#p2344.

[6] Крылова Н.Е. Уголовное право зарубежных стран. Общая и Особенная части. Учебник для магистров / под ред. Н.Е. Крыловой. М.: «Юрайт», 2013. С. 893.

Объективная сторона преступления состоит в одном из следующих альтернативных действий - создание неправильных программ, использование неправильных или неполных данных, неправомочное использование данных, неправомерное воздействие на процесс обработки информации. Состав преступления является материальным. Это значит, что для квалификации необходимо наступление общественно-опасных последствий. Особенность заключается в том, что диспозиция нормы включает в себя два последствия – промежуточное и итоговое. Промежуточным последствием является влияние на результат обработки данных. Итоговым же последствием считается причинение имущественного ущерба.[7]

В связи с наличием большого количества отягчающих обстоятельств, в данной статье, одним из которых является злоупотребление своими полномочиями или своим положением, являясь должностным лицом, или фальсификация наступления страхового случая, если для этой цели он или другое лицо похищает вещь, имеющую значительную стоимость, или полностью или частично разрушает ее посредством поджога, или топит корабль, или сажает его на мель, мы можем сделать вывод о том, что субъектом преступления может быть как общим, так и специальным.

Субъективная сторона компьютерного мошенничества включает в себя прямой преступный умысел и корыстное побуждение, представляющее собой намерение создать для себя или третьего лица противоправную имущественную выгоду.

Несмотря на то, что в Уголовном кодексе Франции, принятом в 1992г. и вступившем в силу в 1994г., включено большое количество преступных деяний в сфере компьютерной информации, отдельного состава компьютерного мошенничества не выделяется. Но, подробно изучив УК Франции можно сделать вывод о том, что уголовные нормы защищают информационные системы и программное обеспечение как объекты

[7] Харламов Д.Д. Уголовная ответственность за компьютерное мошенничество по УК российской Федерации и ФРГ // Проблемы экономики и юридической практики. 2015. №4. С.58.

собственности.[8] Также, одной из особенностей французского уголовного законодательства является то, что субъектами ответственности за преступления в компьютерной сфере могут являться юридические лица.

Согласно Уголовному кодексу Испании, который был принят в 1995 г. и вступил в силу в 1996 г., и структурно состоит из трех книг, компьютерное мошенничество содержится в разделе под названием «Преступления против собственности и социально-экономического порядка» и специальной главе 4 под названием «Об обманном присвоении чужого имущества», где сформулированы различные виды мошенничества.[9] Компьютерное мошенничество не выделяется в отдельную статью, а также как и в УК Швеции, а закреплена во второй части нормы о мошенничестве. В соответствии с санкцией ст. 249 УК Испании предусматривается наказание в виде лишения свободы на срок от 6 месяцев до 3 лет, если сумма хищения превышает 400 евро. Особенность объекта преступного посягательства состоит в том, что им является не только собственность лица, но и социально-экономический порядок. Также в УК Испании содержится расширенный список отягчающих обстоятельств, например, если деяние осуществляется в отношении вещей первой необходимости, жилья или другого имущества, которое имеет особую социальную ценность, если деяние совершается против объектов художественной, культурной или научной ценности и т.д.

Ст. 148а Уголовного кодекса Австрии предусматривает ответственность за материальный ущерб, причиненный лицом с целью получения незаконной выгоды, путем влияния на процессы автоматизированной обработки данных с помощью специальных программ, ввода, изменения или удаления данных или любым другим способом, влияющим на обработку данных. Также как и в УК ФРГ, Швеции, Финляндии, Испании, объективная сторона данного преступного деяния

[8] Уголовный кодекс Франции [Электронный ресурс] // Режим доступа: http:// constitutions.ru/archives/5854.
[9] Уголовный кодекс Испании. [Электронный ресурс] // Режим доступа: http://legislationline.org/documents/section/criminal-codes.

состоит ряда альтернативных действий. Состав являяется материальным, так как ответственность по данной статье наступает только в случае нанесения ущерба. Основной состав этого преступления наказывается лишением свободы на срок до шести месяцев или штрафом до 360 дневных ставок. В случае  за компьютерное мошенничество регулируется статьей 147 Уголовного кодекса Швейцарии. При этом часть 1 данной статьи устанавливает ответственность за совершенное в противоправных целях некорректное и (или) неправомерное использование компьютерной информации в незаконных целях (в интересах себя или кого-то другого), в результате чего собственнику или иному владельцу имущества причиняется вред. Санкцией является штраф или лишение свободы на срок до 5 лет. Таким образом, данное действие представляет собой особый способ причинения материального ущерба с использованием компьютерных данных. Ответственность за соблюдение этого закона из корыстных соображений , регулируется частью второй. Соответственно наказание составляет до 10 лет лишения свободы. Согласно части 3 этой статьи уголовное дело по факту компьютерного мошенничества, совершенного физическим лицом в отношении члена его семьи, осуществляется только по заявлению потерпевшего.

Ответственность за данное преступление по Уголовному кодексу Болгарии закрепляется в статье 212а главы 5 «Преступления против собственности ». В соответствии с ч. 1 ст. 212а, если человек из корыстных побуждений вводит кого-либо в заблуждение, вводя, изменяя или удаляя компьютерные данные или с помощью подделки электронной подписи, он будет наказан за компьютерное мошенничество в виде лишения свобода от 1 до 6 лет со штрафом в размере до 6000 болгарских левов.

Отличительной особенностью данного состава является включение в объективную сторону подделки электронной подписи.

В Уголовном кодексе Республики Польша преступления, совершенные с использованием компьютерной информации и компьютерных технологий

содержатся в специальном разделе 33 «Преступления против сохранности информации».[10] Соответственно, объектом преступлений будет являться сохранность информации. Но, рассматриваемый нами состав, содержится в другом разделе, потому что согласно уголовной доктрине Республики Польша, объектом компьютерного мошенничества являются отношения собственности. Согласно статье 287 УК РП, действие лица признается особым преступлением против собственности, которое с целью получения материальной выгоды или причинения вреда другому лицу без право на это, влияет на автоматизированное преобразование, сбор или передача информации или изменение, аннулирование или создание новой записи в электронном формате» Санкцией данной статьи является наказание в виде лишения свободы от 3 месяцев до 5 лет.

Норма о мошенничестве в сфере компьютерной информации содержится в § 1 ст. 287 раздела 35 «Преступления против собственности». УК РП и трактуется, как хищение путем мошенничества, если это сопровождалось уничтожением, изменением, модификацией или копированием компьютерной информации – наказывается лишением свободы на срок от 3 месяцев до 5 лет с возмещением суммы причиненного ущерба.

Далее, рассмотрим страны англо-саксонской правовой семьи, а именно Великобританию и Соединенные Ш.таты Аме.рики. Вспомним отличительные особенности данной правовой системы. Судебный прецедент выступает основным источником права, отсутствует деление права на частное и публичное, отрасли права структурно не выделяются.[11]

Соединенные Штаты Америки (далее США) явились первым государством, в котором возникла киберпреступность. Еще в далеком 1977 г. в США был разработан законопроект о защите федеральных компьютерных систем. Данный закон закреплял ответственность за ряд преступлений, таких как незаконное использование компьютерных устройств, введение заведомо

[10] Уголовный кодекс Республики Польша [Электронный ресурс] – Режим доступа: http://www.polskieustawy.com/print.php?actid=474&lang =48&adate=20151024&page=4

[11] Рассказов Л.П. Англосаксонская правовая семья: генезис, основные черты и важнейшие источники // Научный журнал КубГАУ. 2015. №.105. С. 14.

ложных данных в компьютерную систему и т.д.. На основании этого закона в 1984 г. был принят специальный закон о мошенничестве и злоупотреблении с использованием компьютеров. Данный правовой акт стал основным закрепленным источником, регулирующим преступления в сфере компьютерной информации. После большого количества изменений и дополнений, в связи со спецификой объекта преступного посягательства, закон был включен в виде §1030 в титул 18 Свода законов США[12].

Так, по мнению Мазурова В.А. «следует отметить, что данный закон устанавливает ответственность за деяния, предмет посягательств которых «защищенный компьютер» (имеющаяся в нем информация). Под ним понимается компьютер, находящийся в исключительном пользовании правительства или финансовой организации, либо компьютер, функционирование которого было нарушено при работе в интересах правительства или финансовой организации, а также компьютер, являющийся частью системы или сети, элементы которой расположены более чем в одном штате США. Закон закрепляет, что уголовная ответственность наступает в случаях несанкционированного доступа (когда посторонний по отношению к компьютеру или компьютерной системе человек вторгается в них извне и пользуется ими) либо превышения санкционированного доступа (когда законный пользователь компьютера или системы осуществляет доступ к компьютерным данным, на которые его полномочия не распространяются)».[13] В данном законе предусматривается ответственность за семь составов преступления, двумя из которых является мошенничество:

- мошенничество с использованием компьютера - доступ, осуществляемый с мошенническими намерениями, и применение компьютера с целью

[12] Свод законов США [Электронный ресурс] – Режим доступа: http://law.justia.com/codes/us/2012/title-18/part-i/chapter-47/section-1030/

[13] Мазуров В.А. Компьютерные преступления: анализ уголовного законодательства США и Германии // Известия АлтГУ. 2005. №2. С.60.

получения чего бы то ни было ценного посредством мошенничества, включая незаконное использование машинного времени стоимостью более 5 тыс. долл. в течение года, т.е. без оплаты эксплуатации компьютерных сетей и серверов;

- мошенничество путем торговли компьютерными паролями или аналогичной информацией, позволяющей получить несанкционированный доступ, если такая торговля влияет на торговые отношения между штатами и с другими государствами или на компьютер, используемый правительством США (§1030 «а», «б»);

## 1.2 Уголовное законодательство стран Содружества Независимых Государств

После распада СССР, за столь недолгое время существования СНГ было принято большое количество нормативно-правовых актов, в том числе были приняты новые уголовные кодексы. В силу общих исторических истоков СНГ перенимает многие положения из законодательства РФ.

Из всех стран СНГ Республика Беларусь первая закрепила ответственность столь необычным образом, в сравнении с другими государствами. В белорусском уголовном законодательстве выделяется девять компьютерной техники. Белорусские законодатели использует более общий подход, чем европейские. Обратимся к статье 212 УК РБ.[14] Она гласит о том, что хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на компьютерных носителях или передаваемой по сетям передачи данных, либо путем внесения ложной информации в компьютерную систему, влечет наложение штрафа, или лишением права занимать определенные должности, или заниматься определенной деятельностью, или арестом на срок до шести месяцев, или ограничением свободы.

[14] Уголовный кодекс Республики Беларусь [Электронный ресурс] - Режим доступа: https://kodeksy-by.com/ugolovnyj_kodeks_rb.htm

Исходя из диспозиции нормы, компьютерная техника выступает в качестве средства совершения хищения. Особенность объективной стороны преступления, предусмотренного ст. 212 УК РБ, заключается в способе нарушения отношений собственности, а именно, либо путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации. Необходимо также наступление общественно-опасного последствия в виде причинения реального ущерба собственнику и завладение чужим имуществом виновным.

Указанная статья находится в главе 24 «Преступления против собственности» соответственно, основным объектом данного преступного посягательства являются отношения собственности, а предметом преступления соответственно имущество. Именно по этой причине, рассматриваемый нами состав преступления по УК РБ не входит в главу 31 «Преступления против информационной безопасности». [15]

Сравнивая УК РБ с вышеупомянутыми уголовными кодексами других государств, можно выделить особенность. Она заключается в том, что в УК РБ не включено понятие «компьютерного мошенничества», или «мошенничества в сфере компьютерной информации». Статья 212 УК РБ называется «хищение путем использования компьютерной техники» и рассматривается как отдельная форма хищения, соответственно включает в себя больше видов преступных посягательств. Аналогичную норму из всех стран, входящих в Содружество Независимых Государств перенял Уголовный кодекс Республики Армения, закрепив в ст.181 главы «Преступления против собственности, экономики и экономической деятельности» норму о хищении, совершенном с использованием компьютерной техники. Диспозиция нормы значительно короче, чем в УК

[15] Гриб Д.В. Хищение имущества путем использования информационных технологий в Уголовном кодексе Российской Федерации и Республики Беларусь: сравнительный аспект // Вестник Московского университета МВД России. 2019. №4. С. 75.

РБ, и трактуется как хищение чужого имущества в значительных размерах, совершенное с использованием компьютерной техники.

В главе 6 Уголовного кодекса Казахстана, принятого в июле 1997г. выделяется отдельная статья о мошенничестве.[16] Также как и в уголовном законодательстве Республики Беларусь, мошенничество не разделено по видам. В соответствии с п.4 ч.2 статьи 190 УК РК квалифицирующим признаком мошенничества является мошенничество путем обмана или злоупотребления доверием пользователя информационной системы. Выделение данного состава в ч.2 ст.190 УК РК обусловлено повышенной общественной опасностью преступлений против собственности с использованием информационных технологий и технических средств.[17] Следовательно, мы можем сделать вывод о том, что в УК РК отсутствует отдельная статья о мошенничестве в сфере компьютерной информации.

Указание на ввод, удаление, блокирование компьютерной информации и иное вмешательство в УК Казахстана, в отличие от УК России, отсутствует.

Остальные страны СНГ, на данный момент фактически не содержат каких-либо специальных положений относительно компьютерного мошенничества. Государства используют в правоприменительной практике нормы о мошенничестве и отдельные статьи о преступлениях в сфере компьютерной информации.

Таким образом, проанализировав законодательство европейских стран, США и страны СНГ можно сделать ряд выводов. Большое количество государств своевременно реформирует уголовное законодательство и включает в него ответственность за новый вид мошенничества. Единое определение компьютерного мошенничества отсутствует. Сравнительный

---

[16] Уголовный кодекс Республики Казахстан / Закон Республики Казахстан от 16 июля 1997 года № 167 (Ведомости Парламента РК, 1997 г., № 15-16, ст. 211) / Предисловие министра юстиции Республики Казахстан, докт. юрид. наук, проф. И.И. Рогова. СПб.: Изд-во «Юридический центр Пресс», 2001. С.232.

[17] Чечель Г.И., Третьяк М.И. Законодательная регламентация преступлений против собственности в сфере высоких технологий в УК Казахстана и России // Всероссийский криминологический журнал. 2018. №1. С. 229.

анализ составов преступления в разных странах показал, что в некоторых странах состав является материальным (Испания, Швейцария и т.д.), в некоторых (Болгария и т.д.) формальным. Основным объектом преступного посягательства во всех рассмотренных государствах выступают отношения собственности, так как преступления находятся в разделах «Преступления против собственности». В некоторых странах также выделяются дополнительные объекты, такие как социально-экономический порядок, нормальное функционирование компьютерных систем. В ряде стран, мошенничество в сфере компьютерной информации выделяется в отдельную статью (ФРГ и т.д.), в остальных же она является квалифицированным составом простого мошенничества, либо приравнивается к нему. Субъективная сторона преступления характеризуется прямым умыслом и практически во всех рассмотренных странах обладает специальной целью. Она состоит в намерении незаконно обогатиться самому виновному или обогатить третье лицо. Преобладающими санкциями за совершение мошенничества сфере компьютерной информации, являются штраф и лишение свободы. При этом срок лишения свободы варьируется в зависимости от отягчающих обстоятельств от нескольких месяцев до 10 лет.

# Глава 2. Уголовно-правовой анализ состава преступления, предусмотренного ч.1 ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации»

## 2.1 Объект мошенничества в сфере компьютерной информации

Состав преступления является системой, предусмотренных уголовным законом объективных и субъективных элементов, признаки которых раскрывают их содержание и характеризуют преступление как общественно опасное и уголовно противоправное деяние. Состав преступления содержит в себе четыре элемента – объект, субъект, объективную сторону и субъективную сторону. Наличие в совершенном деянии всех вышеуказанных элементов состава преступления является основанием для признания его преступным и в последующем привлечения совершившего его лица к уголовной ответственности. При отсутствии хотя бы одного из них можно сделать вывод об отсутствии состава преступления, в общем и целом, а деяние при таких условиях так же не признается преступным. При рассмотрении конкретного состава преступления и вопросов, касающихся квалификации, на первоначальном этапе предполагает анализ его объекта.

В действующем Уголовном кодексе Российской Федерации не содержится четкого определения объекта преступления, именно поэтому в настоящее время в теории уголовного права актуальным остается вопрос о том, что понимается под «объектом преступления». Исходя из этого, в уголовно-правовой литературе выделяется два ключевых подхода к толкованию понятия объекта преступления.

Традиционно, первый подход гласит, что в российском уголовном праве объектом преступного деяния принято считать охраняемую уголовным законом систему общественных отношений между людьми, которым в свою очередь причиняется вред в результате совершения преступления, или создается угроза причинения вреда.

Как отмечалось в учебнике А.В. Бриллиантова, «ставшая уже традиционной трактовка и восприятие объекта преступления как совокупности общественных отношений, то есть отношений между людьми, в какие бы сложные формы они не воплощались, и сегодня продолжает оставаться господствующей».[18]

Всех сторонников второго подхода объединяет одно: критическое восприятие идеи о том, что объектом преступления выступают общественные отношения и только они. Так, согласно позиции А.В. Наумова «объектом преступления может рассматриваться лишь то, что терпит ущерб в результате преступления, а именно блага (интересы), на которое посягает преступное деяние и которые охраняются уголовным законом».[19] Более широко объект преступления рассматривает Т.А. Бушуева. По ее мнению объект преступления – это блага, интересы, общественные отношения, которые охраняются уголовным законом.[20]

Весьма интересная точка зрения была высказана Г.П. Новоселовом, который определял объект как «…тот, против кого совершается преступление, т.е. отдельное лицо или некое множество лиц, материальные или нематериальные ценности, которых, будучи поставленными под уголовно-правовую охрану, подвергаются преступному воздействию, в результате чего этим лицам причиняется вред или создается угроза причинения вреда».[21]

В данной работе я руководствовалась мнением, о том, что объектом преступления все-таки является только совокупность общественных отношений, т.к. данная позиция является наиболее распространенной и устоявшейся.

---

[18] Бриллиантов А.В. Уголовное право России. Части Общая и Особенная: учеб. / под ред. А.В. Бриллиантова. М.: «Проспект», 2010. С. 95.
[19] Наумов А.В. Уголовное право. Общая часть. М.: «Норма», 1999. С. 121.
[20] Бушуева Т.А., Дагель П.С. Объект уголовно-правовой охраны природы // Советское государство и право. 1977. № 8. С. 80.
[21] Уголовное право. Общая часть / под ред. И.Я. Козаченко. М.: «Норма», 2008. С. 212.

В российской уголовно-правовой доктрине принято выделять следующие виды объектов преступления: общий, родовой, видовой, непосредственный. Кратко рассмотрим каждый из вышеупомянутых видов.[22]

Общий объект преступления – это вся совокупность (система) общественных отношений, охраняемых государством посредством норм уголовного права. Общим объектом состава преступления, предусмотренного ст.159.6 УК РФ является вся охраняемая уголовным законом система социально значимых общественных отношений, отражающую содержание социальных благ, по поводу которых существуют эти отношения.[23] Система охраняемых наиболее социально значимых отношений в общем виде представлена в ст. 2 УК РФ «Задачи Уголовного кодекса Российской Федерации».

Родовым объектом является группа однородных или тождественных общественных отношений, охраняемых уголовным законом от преступных посягательств.[24] Именно эти отношения являются критерием, который кладется в основу построения Особенной части УК, разделенной на разделы, в зависимости от родового объекта.

Анализируемая норма о мошенничестве в сфере компьютерной информации содержится в Разделе VIII «Преступления в сфере экономики», следовательно родовым объектом данной нормы выступают общественные отношения, возникающие в сфере экономики, которая представляет из себя систему производства, распределения, обмена и потребления товаров и услуг.[25] Таким образом, экономика воспринимается через систему экономических процессов, складывающихся в обществе на основе имущественных отношений и политических систем.[26] Именно данная позиция нашла свое отражение в доктринальных источниках.

---

[22] Уголовное право Российской Федерации. Общая часть / под ред. Л.В. Иногамовой-Хегай, А.И. Рарога, А.И. Чучаева. М.: «ИНФРА-М- КОНТРАКТ», 2011. С. 105.
[23] Барчуков В.К. К проблеме определения родового и видового объекта состава преступления, предусмотренного ст. 159.6 УК РФ // Пробелы в российском законодательстве. 2016. № 7. С. 161.
[24] Уголовное право. Общая часть: учебник / под ред. И.Я. Козаченко. М.: «Норма», 2008. С. 263.
[25] Борисов Е.Ф. Экономическая теория: Учебник. 3-е изд., перераб. и доп. М.: «Юрайт», 2005. С. 182.
[26] Экономика: учебник / под ред. доц. А.С. Булатова. М.: «Бек», 1995. С.408

Вместе с тем, следует отметить, что понятие «сфера экономики» не однозначно воспринимается в науке уголовного права, что вызывает определенную дискуссионность этого вопроса, актуализирующуюся на следующем уровне познания объекта рассматриваемой нормы - видовом объекте.

Видовой объект выступает частью родового объекта и в свою очередь объединяет более узкие группы отношений. Он соотносится с родовым объектом как часть с целым, как вид с родом. Именно с учетом этих отношений статьи объединяются в главы УК РФ.

Исследуемая норма о компьютерном мошенничестве входит в главу 21 «Преступления против собственности» и является специальной по отношению к общей статье о мошенничестве, закрепленной в ст. 159 УК РФ. Из этого следует, что видовым объектом у данного состава преступления является совокупность общественных отношений собственности. В уголовном праве РФ собственности присуще экономико-правовое (комплексное) понимание. В уголовно-правовом смысле указанной категорией охватываются: а) собственнические отношения (общественные отношения, складывающиеся в связи с реализацией права владения, пользования и распоряжения имуществом, находящимся в частной, государственной, муниципальной и иной формы собственности граждан и юридических лиц, а также Российской Федерации, субъектов Российской Федерации, муниципальных образований); б) другие вещные отношения (общественные отношения, складывающиеся в связи с реализацией таких вещных прав, как право хозяйственного ведения имуществом, право оперативного управления имуществом, сервитуты и др.); в) обязательственные отношения (общественные отношения, складывающиеся в силу возникновения договорных и иных обязательств, когда одно лицо (должник) обязано совершить в пользу другого лица (кредитора) определенное действие, как то: передать имущество, выполнить работу, оказать услугу, внести вклад в совместную деятельность, уплатить деньги и

т.п., либо воздержаться от определенного действия, а кредитор имеет право требовать от должника исполнения его обязанности); г) иные имущественные отношения.

Непосредственный объект представляет собой то конкретное общественное отношение, которое поставлено под охрану конкретной уголовно-правовой нормой и при нарушении которой происходит причинение вреда такому отношению. Стоит согласиться с мнением Т.Д. Устиновой о том, что «... если продолжить далее линию о важности установления непосредст- венного объекта данного элемента состава преступления, то это не только приводит к правильной квалификации содеянного, т.е. установлению тождества между содержанием признаков состава в уголовно-правовой норме и совершенным деянием, но и оказывает существенное влияние на всю дальнейшую судьбу лица, виновного в совершении преступления».[27] В качестве основного непосредственного объекта компьютерного мошенничества необходимо рассматривать конкретные общественные отношения в области охраны собственности.[28]

Непосредственный объект может быть основным, дополнительным и факультативным. Дополнительным объектом признается общественное отношение, которому причиняется вред в связи, попутно, с причинением вреда основному объекту.[29]

В науке уголовного права ведутся споры относительно выделения иного непосредственного объекта преступления предусмотренного 159.6 УК РФ. Единого понимания учеными на данный момент не достигнуто. Дискуссия возникла из-за того, что законодатель включил в норму указание на сферу компьютерной информации.

Интересна позиция В.И. Гладких о том, что рассматриваемая норма нерезонно включена в Раздел VIII «Преступления против собственности». Он

[27] Устинова Т.Д. Уголовная ответственность за лжепредпринимательство / по ред.Т.Д. Устиновой. М.: «Норма», 2003. С. 51.
[28] Барчуков В.К. Непосредственный объект мошенничества в сфере компьютерной информации // Пробелы в российском законодательстве. 2018. №7. С. 260.
[29] Уголовное право. Общая часть.: учебник / под ред. А.Н. Тарбагаева. М.: «Проспект», 2012. С.105.

считает, что мошенничество в сфере компьютерной информации предполагает в качестве основного непосредственного объекта отношения в сфере обеспечения информационной безопасности.[30]

Ряд известных ученых придерживается позиции о том, что норма закрепленная в ст. 159.6 УК РФ является двуобъектной. Так, по мнению Сафонова О. М. из самого названия нормы следует, что дополнительным объектом являются отношения в сфере безопасности компьютерной информации.[31] Лопатина Т.М. отмечает, что общественные отношения в сфере компьютерной информации выступают факультативным объектом и совершение преступления предусмотренного ст. 159.6 УК РФ не всегда влечет угрозу причинения вреда компьютерной безопасности.[32]

Рассмотрев различные точки зрения ученых по поводу непосредственного объекта компьютерного мошенничества, можно сделать вывод о том, что выделение основного и дополнительного непосредственного объекта является наиболее целесообразным, т.к. рассматриваемая норма является специфичной и посягает не только на отношения собственности, но и на общественные отношения в сфере компьютерной информации.

В таком случае, судам необходимо обратить внимание на то, что необходимо осуществлять уголовно-правовую охрану дополнительного объекта, составляющего общественные отношения в сфере компьютерной информации. На этот факт даже указывает Верховный Суд Российской Федерации. В соответствии с п. 22 Постановления от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» Верховный Суд РФ пояснил, что «мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к

[30] Гладких В.И. Компьютерное мошенничество: а были ли основания его криминализации? // Российский следователь. 2014. №22. С. 29.
[31] Сафонов О.М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: дис. ... канд. юрид. наук. М, 2015. С. 115.
[32] Лопатина Т.М. Проблемы уголовно-правовой защиты сфер компьютерной информации: современный взгляд на мошенничество // Право и безопасность. 2013. №3 (45). С. 93.

компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по статье 272, 273 или 274.1 УК РФ.[33] Из данных разъяснений можно сделать вывод о том, что отношения в сфере компьютерной информации являются факультативным объектом, т.к. не всегда подвергаются посягательству.

Не является до конца решенным вопрос относительно предмета мошенничества в сфере компьютерной информации.

В теории уголовного права существует несколько подходов по поводу определения предмета преступления. Первый подход заключается в том, что под предметом понимают только лишь материальные вещи внешнего мира, посредством воздействия на которые, преступник причиняет вред охраняемым общественным отношениям.[34]

Вторая точка зрения заключается в том, что помимо материальных вещей в предмет так же входят иные объекты имущественных отношений в той части, в какой они составляют экономическую ценность, имеют стоимостное выражение и подлежат денежной оценке. То есть к иным объектам можно отнести информацию, энергию, имущественные права, интеллектуальные ценности. Таким образом предмет преступления определяется как материальные и нематериальные блага, которым причиняется или создается угроза причинения вреда преступным воздействием. Данная позиция представляется более рациональной и верной, так как для компьютерного мошенничества как раз-таки в качестве предмета характерны не только материальные блага.

Н. А. Беляев, как известно, настаивал на том, что в качестве предмета посягательства может выступать каждый из элементов общественного отношения, охраняемого уголовным законом, вне зависимости от того,

---

[33] 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.

[34] Уголовное право Российской Федерации. Общая часть / под ред. Л.В. Иногамовой-Хегай, А.И. Рарога, А.И. Чучаева. М.: «ИНФРА-М- КОНТРАКТ», 2011. С. 128.

материальный он или идеальный. Вещи, физические и юридические лица, а также их деятельность и даже сам преступник могут выступать в качестве предмета посягательства.[35]

М. Ю. Дворецкий пишет, что предметом преступного посягательства по ст. 159.6 УКРФ являются: 1) компьютерная информация, под которой в уголовно- правовом аспекте понимаются сведения ( или сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи, согласно положениям примечания к ст. 272 УК РФ; 2) имущество, то есть совокупность вещей, которые находятся в собственности лица, в том числе включая деньги и ценные бумаги, а также имущественные права на получение вещей или имущественного удовлетворения от других лиц.[36]

Противоположной позиции придерживается Т. М. Лопатина, так, по ее мнению, предметом компьютерного мошенничества, как и традиционного мошенничества, является чужое имущество или право на него. Но в компьютерах и компьютерных сетях хранятся не деньги или имущество, а информация о них или об их движении. Информация – это не имущество, она не обладает экономическим, социальным и юридическим признаками, характеризующими чужое имущество как предмет хищения, который выступает обязательным признаком состава мошенничества.[37]

Представляется, что в качестве предмета компьютерного мошенничества, как и любого другого хищения, действительно справедливо рассматривать имущество. Однако специфика рассматриваемого преступления заключается в том, что вещи, как и наличные денежные средства, обладающие вещно-правовой природой, хотя и могут выступать предметом, но не типичны для данного вида мошенничества. Практика показывает, что предметом посягательства при компьютерном

[35] Беляев Н.А. Курс советского уголовного права. Часть общая / под ред. Н.А. Беляева, М.Д. Шаргородского. Л.: «Изд-во Ленингр. ун-та», 1968. С. 110.
[36] Дворецкий М.Ю. Уголовная ответственность за мошенничество в сфере компьютерной информации: проблемы теории и правоприменительной практики // Вестник ТГУ. 2013. №8. С. 409.
[37] Лопатина Т.М. Проблемы уголовно-правовой защиты сфер компьютерной информации: современный взгляд на мошенничество // Право и безопасность. 2013. №3 (45). С. 89-95.

мошенничестве, как правило, выступают безналичные и электронные деньги, а также новые виды цифровых финансовых активов к которым можно отнести виртуальную валюту и криптовалюту.[38]

Дискуссионным является вопрос о возможности отнесения к предмету мошенничества в сфере компьютерной информации премиальных денежных суррогатов, возникающих в связи с реализацией разнообразных программ потребительской лояльности (бонусы, баллы, подарочные мили и т. п.). Обозначенная проблема интересна не только в теоретическом плане, но и обусловлена прикладными потребностями. В судебно-следственной практике можно встретить решения, связанные с оценкой подобных противоправных действий с премиальными денежными суррогатами.[39]

Так, М., являясь оператором телефонного центра ООО « Директ Стар», которое выполняет для ОАО «Аэрофлот» функции контакт-центра по обслуживанию пассажиров, используя доступ к информационной системе «Аэрофлот Бонус», создал более 10 фиктивных счетов на имя вымышленных лиц, посредством чего неправомерно накапливал бонусные мили за счет полетов пассажиров, не являющихся участниками программы. В дальнейшем М. через сеть «Интернет» предложил тридцати одному клиенту за значительно меньшую оплату возможность приобретения бонусных авиабилетов ОАО «Аэрофлот». В результате действий М. по незаконному накоплению бонусных миль и приобретению за их счет премиальных авиабилетов ОАО «Аэрофлот» был причинен имущественный ущерб на сумму 1345675 рублей 35 копеек. Решением суда М. признан виновным по п. «б» ч. 2 ст. 165 УК РФ.[40]

Я считаю, что суд совершенно обоснованно квалифицировал действия виновного как причинение имущественного ущерба путем обмана. Так как у

[38] Савельев А. И. Электронная коммерция в России и за рубежом: правовое регулирование. 2-е изд. М.: «Статут», 2016. С. 40.
[39] Фролов М.Д. К вопросу о мошенничестве в сфере компьютерной информации // Образование и право. 2018. №3. С. 180.
[40]Приговор Ленинского районного суда г. Владимира [Электронный ресурс] : приговор от 08.03.2013 по делу № 1-78/2013 // Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). – Режим доступа: https://sudact.ru/

ОАО «Аэрофлот» не изымали имущество, а путем использования правил программы бонсных авиабилетов не доплатили за оказанные услуги, то есть реальный ущерб выразился в неполучении должного.

Вместе с тем, в тех случаях, когда подобные бонусные мили (баллы), предоставляющие возможность оплаты ими всей или части покупки, обладают способностью к обороту, то есть могут отчуждаться третьим лицам, а значит и выступать предметом преступного посягательства против собственности, такие премиальные (дисконтные) денежные суррогаты, могут выступать в том числе и предметом мошенничества в сфере компьютерной информации.

Таким образом, рассмотрев различные подходы к пониманию объекта компьютерного мошенничества можно сделать вывод, что преступление, предусмотренное ст.159.6 УК РФ является двуобъектным. Основным непосредственным объектом являются отношения собственности, а факультативным дополнительным – отношения в сфере безопасности компьютерной информации.

## 2.2 Объективная сторона мошенничества в сфере компьютерной информации

Объективная сторона преступления есть процесс общественно опасного и противоправного посягательства на охраняемые законом интересы, рассматриваемый с его внешней стороны, с точки зрения последовательного развития тех событий и явлений, которые начинаются с преступного действия (бездействия) субъекта и заканчиваются наступлением преступного результата.[41] Ее образуют признаки, характеризующие сами по себе акт волевого поведения человека, протекающего в объективном мире: деяние (действие или бездействие), общественно опасное последствие,

[41] Уголовное право. Общая часть.: учебник / Под ред. А.Н. Тарбагаева. М.: «Проспект», 2012. С.108.

способ, место, время, обстановка, орудие и средства совершения преступления.[42]

Российский уголовный закон определяет мошенничество в ч. 1 ст. 159 УК РФ как «хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием».[43] Из действующей редакции нормы следует, что мошенничество может существовать в двух относительно самостоятельных формах: как хищение чужого имущества и как приобретение права на чужое имущество. На это же обращает внимание Г.В. Слепова: «диспозиция ст. 159 УК РФ содержит два самостоятельных элемента: хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием».[44] Эти элементы, как называет их Г.В. Слепова, отделены друг от друга разделительным союзом «или», что также указывает на их самостоятельность и обособленность.

Согласно примечанию к ст. 158 УК РФ под хищением понимаются совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества.[45]

Приобретение права на чужое имущество представляет собой особую разновидность посягательства на собственность, которая по своей юридической сути не является хищением, так как не связана с непосредственным изъятием и (или) обращением чужого имущества в пользу виновного или других лиц. Специфика данной разновидности мошенничества заключается в том, что лицо, его совершающее, путем обмана или злоупотребления доверием не завладевает имуществом, а лишь приобретает право на него. По существу, речь идет о юридическом способе

[42] Там же.
[43] Уголовный кодекс Российской Федерации. [Электронный ресурс] : федер. закон от 13.06.1996 № 63-ФЗ ред. от 31.07.2020 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.
[44] Слепова Г.В. Дискуссионные подходы к поня- тию «право на имущество» в теории уголовного права // Вестник Калининградского юридического института МВД России. 2011. № 2 (24). С. 128.
[45] Там же.

изъятия, в отличие от физического, о котором идет речь в примечании 2 к ст. 158 УК РФ.

С точки зрения законодателя приобретение права на имущество не равнозначно приобретению имущества. Так, обладатель права на имущество для того, чтобы приобрести само имущество, должен совершить еще другие, дополнительные действия. При этом лицу, противоправно приобретшему право на имущество, в том числе путем обмана или злоупотребления доверием, собственник либо иной владелец данного имущества может воспрепятствовать в реализации этого права путем обращения, например, в правоохранительные или иные государственные органы.

Понятие «приобретение права на чужое имущество» подразумевает под собой оформление права собственности на вещь либо приобретение обязательственного права, которое позволяет завладеть этой вещью в будущем. При этом, в последней части объективная сторона преступления оказывается сконструированной по типу формального состава, отличаясь тем самым от хищения моментом окончания.

Ю. И. Ляпунов, придерживаясь аналогичной позиции, также исходит из того, что закрепление права на имущество в различных документах (завещании, страховом полисе, доверенности на получение тех или иных материальных ценностей) предопределяет то обстоятельство, что при получении мошенником документов, на основании обладания которыми он приобретает право на имущество, преступление считается оконченным, независимо от того, удалось ли мошеннику получить по ним соответствующее имущество.

По конструкции объективной стороны состав мошенничества в сфере компьютерной информации является материальным и считается оконченным с момента, когда указанное имущество поступило в незаконное владение виновного или других лиц и они получили реальную возможность (в зависимости от потребительских свойств этого имущества) пользоваться или распорядиться им по своему усмотрению, но согласно Постановлению

Пленума Верховного Суда РФ от 30 ноября 2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», что если предметом преступления при мошенничестве являются безналичные денежные средства, в том числе электронные денежные средства, то по смыслу положений пункта 1 примечаний к статье 158 УК РФ и статьи 128 Гражданского кодекса Российской Федерации содеянное должно рассматриваться как хищение чужого имущества. Такое преступление следует считать оконченным с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которого владельцу этих денежных средств был причинен ущерб.[46]

Соответственно, в законе закреплены разные моменты окончания мошенничества – в форме хищения и в форме приобретения права на имущество: как момент получения виновным реальной возможности пользоваться или распорядиться имуществом по своему усмотрению и как момент возникновения у виновного юридически закрепленной возможности вступить во владение или распорядиться чужим имуществом как своим собственным.

Объективная сторона анализируемой нормы обладает уникальностью, т.к. характеризуется специфичными способами совершения преступления, а именно путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Терминология, используемая в диспозиции нормы, схожа с терминологией диспозиций норм, содержащихся в главе 28 УК РФ «Преступления в сфере компьютерной информации». Так, согласно примечанию 1 к ст. 272 УК РФ под компьютерной информацией понимаются

[46] 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.

сведения, представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. В соответствии со ст.2с Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информационно-телекоммуникационная сеть – это технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.[47]

В российской уголовно-правовой науке на данный момент отсутствует единое понимание и представление о содержании признаков объективной стороны преступления предусмотренного ст. 159.6 УК РФ, т.к. анализируя объективную сторону компьютерного мошенничества, можно сделать вывод о том, что в отличии от общей нормы о мошенничестве, мошенничество в сфере компьютерной информации не содержит в себе указания на такой способ совершения преступления как обман и злоупотребление доверием. Согласно Постановлению Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» обман как способ совершения хищения или приобретения права на чужое имущество может состоять в сознательном сообщении (представлении) заведомо ложных, не соответствующих действительности сведений, либо в умолчании об истинных фактах, либо в умышленных действиях (например, в предоставлении фальсифицированного товара или иного предмета сделки, использовании различных обманных приемов при расчетах за товары или услуги или при игре в азартные игры, в имитации кассовых расчетов и т.д.), направленных на введение владельца имущества или иного лица в заблуждение.[48]

В доктринальном понимании классического мошенничества под обманом понимается намеренное введение в заблуждение лица относительно

[47] Об информации, информационных технологиях и о защите информации [Электронный ресурс] : федер. закон от 27.07.2006 № 149-ФЗ ред. от 08.06.2020 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

[48] 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.

каких-либо обстоятельств фактов либо сознательное умолчание о них в нарушение правовой обязанности. Искажаться могут любые факты, о личности мошенника, о наличии у него в собственности какого-либо имущества, о его планах на предпринимательскую или трудовую деятельность, о свойствах имеющихся у него в распоряжении вещей и т.д.[49]

Стоит согласиться с мнением Д.В. Шебанова который отмечает, что «ни о каком обмане либо злоупотреблении доверием в диспозиции рассматриваемой статьи речи не идет. И это логично - ведь обмануть машину, то есть бездушную вещь, лишенную психики, невозможно. Чем, прежде всего, отличалось традиционное мошенничество - прямым или виртуальным, но обязательно контактом с живым лицом. В предложенной законодателем норме это становится неактуальным».[50]

Т. М. Лопатина также отмечает, что указание на «обман и злоупотребление доверием» неприменимо к компьютерной системе, которая не имеет интеллекта и воли и не может добровольно передать имущество под влиянием обмана или в результате злоупотребления доверием».[51]

Как справедливо отмечает В. Г. Шумихин в составе мошенничества в сфере компьютерной информации законодатель не указал способ обмана или злоупотребления доверием и, таким образом, он представляет собой самостоятельную форму хищения со специфичным способом, отличным от других форм хищения чужого имущества.[52]

В связи с этим, стоит обратиться к пояснительной записке к проекту Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации». В ней предлагалось выделить в самостоятельный состав преступления мошенничество в сфере компьютерной информации (статья

[49] Бриллиантов А.В. Уголовное право России. Части Общая и Особенная: учеб./ под ред. А.В. Бриллиантова. – Москва : Проспект, 2010. С. 95

[50] Шебанов Д. В. О некоторых проблемах квалификации мошенничества в сфере компьютерной информации // Теория и практика общественного развития. 2014. № 4. С. 241.

[51] Лопатина Т.М. Проблемы уголовно-правовой защиты сфер компьютерной информации : современный взгляд на мошенничество // Право и безопасность. 2013. №3 (45). С. 91.

[52] Шумихин В.Г. Седьмая форма хищения чужого имущества // Вестник Пермского университета. №2 (24). 2014. С. 230.

$159^6$ УК РФ законопроекта), когда хищение или приобретение права на чужое имущество сопряжено с преодолением компьютерной защиты имущества (имущественных прав) и осуществляется путем ввода, удаления, модификации или блокирования компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Подобные преступления совершается не путем обмана или злоупотребления доверием конкретного субъекта, а путем получения доступа к компьютерной системе и совершения вышеуказанных действий, которые в результате приводят к хищению чужого имущества или приобретению права на чужое имущество (определение термина «компьютерная информация» дано в примечании 1 к статье 272 УК РФ как сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средства их хранения, обработки и передачи).[53]

Недаром в Постановлении Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» Верховный Суд «забывает» о том, что речь в ст. 159.6 УК, согласно букве закона, идет о хищении: «По смыслу статьи 159.6 УК РФ вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей признается целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) - ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает

[53] Пояснительная записка к законопроекту № 53700-6 «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» // Система обеспечения законодательной деятельности [сайт]. – Режим доступа: https://sozd.duma.gov.ru.

установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет

виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него.[54]

Соответственно, мы видим, что законодатель пояснил особенность данного вида преступления, но данное пояснение только вызвало ряд вопросов в правоприменительной практике, так как суды столкнулись с совершенно новой формой мошенничества, не обладающей основными признаками, в классическом понимании.

Рассмотрим более подробно альтернативные способы, входящие в диспозицию рассматриваемой нормы. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 31.12.2014) «Об информации, информационных технологиях и о защите информации» не закрепляет и не раскрывает содержание таких терминов как «ввод», «удаление», «блокирование», «модификация» компьютерной информации, но в доктрине уголовного права выработаны разные подходы, определяющие содержание указанных признаков.

Подробно изучив судебную практику по делам о компьютерном мошенничестве, можно сделать вывод о том, что наиболее часто преступление совершается именно путем ввода. Многие ученые предлагают свои варианты раскрытия понятий, входящий в диспозицию анализируемой нормы.

Так, под вводом компьютерной информации, по мнению М.И. Третьяк понимается определенный алгоритм действий по набору данных об адресате (номера его лицевого счета, мобильного телефона, данных мобильного кошелька и др.), сведений о сумме денежных средств (данных о ценной бумаге) и непосредственному переводу их указанному адресату (операции «перевести», «отправить», «исполнить»), далее их обработка, распознание

[54] 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.

компьютерной системой и наступление результата – поступление денежных средств (ценной бумаги) адресату.[55]

Согласно мнению Т. М. Лопатиной под вводом компьютерной информации необходимо понимать «размещение сведений в компьютере для их последующей обработки или хранения».

Необходимо отметить, что описывая в ст. 272 УК РФ одно из последствий неправомерного доступа к компьютерной информации, законодатель использует термин «уничтожение», а не «удаление» (ст. 159.6 УК РФ), что порождает неясность: является ли данный факт опиской, или использование разных терминов связано с их различными определениями?

Анализ подходов к определению признака «уничтожение» компьютерной информации в сравнении с подходами к толкованию признака «удаление» компьютерной информации позволяется сделать вывод, что содержание данных понятий идентично. Я разделяю такую позицию, ее придерживается большинство ученых. Так, под удалением

В настоящее время отсутствует судебная практика, согласно которой компьютерное мошенничество совершенно исключительно путем удаления. В большинстве случаев данное деяние сопряжено с вводом информации.

Так, например, Б. и К. были осуждены за мошенничество в сфере компьютерной информации, совершенное группой лиц по предварительному сговору (ч. 2 ст. 159.6 УК РФ). Б., являясь бухгалтером у индивидуального предпринимателя, из корыстной заинтересованности, с целью хищения денежных средств, находящихся на расчетном счете индивидуального предпринимателя, вступила в преступный сговор с К., работающей главным бухгалтером. Движимые корыстными побуждениями, с целью личной наживы, Б. , в обязанности которой входило начисление заработной платы, действуя в интересах себя лично и К. , в электронном зарплатном файле «Список на перечисление зарплаты» рассчитывала заработную плату по всем

[55] Третьяк М.И. Проблемы квалификации новых способов мошенничества // Уголовное право. 2015. № 2. С. 96.

сотрудникам за фактически отработанное время, где умышленно, с целью исключения последующих удержаний материального характера, невносила сведения о завышенной сумме заработной платы для себя лично и К., однако, в графе «итого» незаконно, умышленно указывала итоговую суммарную сумму в сторону увеличения равную сумме, предназначенной для выплаты себе лично и К. Далее Б. , заведомо зная, что индивидуальный предприниматель не будет пересчитывать итоговую суммарную сумму, представляла вышеуказанный документ в распечатанном виде. Индивидуальный предприниматель, полностью доверяя своим бухгалтерам Б. и К., не подозревая о преступных намерениях последних, подписывала своей цифровой электронной подписью платежное поручение на итоговую суммарную сумму, указанную в графе «итого» документа «Список на перечисление зарплаты», предоставленном Б. и отправляла через автоматизированную систему в банк. В свою очередь банк списывал денежные средства с расчетного счета индивидуального предпринимателя в размере итоговой суммарной суммы, указанной в платежном поручении. После того, как итоговая суммарная сумма зачислялась на корреспондирующий счет для распределения на индивидуальные лицевые счета сотрудников, индивидуальный предприниматель давала команду главному бухгалтеру К. на отправку электронного расчетного файла «Список на перечисление зарплаты», назвав номер платежного поручения. К. на своем персональном рабочем компьютере с установленной автоматизированной программой «Клиент» незаконно, умышленно удаляла значение своей начисленной заработной платы и заработной платы Б. и вводила новое значение увеличенной суммы заработной платы в электронном зарплатном файле «Список на перечисление зарплаты», зная заранее на какую сумму они увеличили итоговую суммарную сумму, посредством электронной цифровой подписи и конфиденциального пароля.

Таким образом, Б. и К. по предварительному сговору похитили денежные средства, принадлежащие индивидуальному предпринимателю,

путем удаления значения начисленной им заработной платы и ввода незаконно

нового значения заработной платы в повышенном размере в выгружаемые файлы автоматизированной системы «Клиент». Данные незаконные действия Б. и К. привели к завышению размера перечисленной заработной платы К. на сумму 500500 рублей, Б. на сумму 506 415 рублей, которые они незаконно получили на свои банковские личные карты, распорядившись ими по своему усмотрению.[56]

Блокирование информации - невозможность получить доступ в течение значимого промежутка времени к компьютерной информации ее законному пользователю при сохранности самой информации в памяти ЭВМ. Разблокирование информации может быть осуществлено как в результате чьих-либо действий, так и автоматически по истечении определенного промежутка времени. Блокирование информации должно продолжаться в течение такого отрезка времени, которого достаточно, чтобы нарушить нормальную деятельность пользователей информации или создать угрозу нарушения этой деятельности.[57] Также, определение данному способу дается в Методических рекомендациях по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. Так, под блокированием информации понимается «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,

[56] Приговор Салаватского городского суда Республики Башкортостан [Электронный ресурс] : приговор от 21.05.2015 по делу № 1-113/2015 // Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). – Режим доступа: https://sudact.ru/

[57] Кочои С.М. Нормы о мошенничестве в УК РФ: особенности и отличия // Всероссийский криминологический журнал. 2013. №4. С. 104.

целенаправленное затруднение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением».[58]

Модификацией являются любые изменения компьютерной информации. Модификация может осуществляться путем как частичной замены первоначальной информации на другую, так и добавления новой информации к первоначальной. Также модификацией будут являться различные нарушения прежнего вида представления информации, как-то: изменение порядка частей в документе (страниц, абзацев, строк), попадание частей одних документов в содержание других документов, нарушение взаимного расположения документов в базе данных, внедрение в текст документов посторонних элементов («мусора»).

В. В. Хилюта определяет модификацию компьютерной информации как внесение в компьютерную информацию любых изменений, которые обусловят ее отличие от ранее хранившейся в компьютерной сети, системе или на машинном носителе собственника информационного ресурса, в результате чего потерпевшему будет причинен имущественный ущерб, а виновное лицо извлечет из этого выгоду.[59] Я считаю, что данное определение является исчерпывающим. Как представляется, принципиальное отличие модификации от ввода заключается в том, что в последнем случае лицо не изменяет какой-то информационный объект (блок), а создает новый.

Так, в офисе обслуживания и продаж ПАО «Вымпелком», расположенном по адресу: РБ, г. Октябрьский, 34 мкр., 8 «а», гражданка Д.В., являясь специалистом офиса обслуживания и продаж в г.Октябрьский ПАО «Вымпелком», имея навыки работы в компьютерной программе «1С», ознакомившаяся с нормативными документами и требованиями по информационной безопасности, имея присвоенный индивидуальный и конфиденциальный логин и пароль, необходимый для

[58] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] // Режим доступа: https://www.garant.ru/products/ipo/prime/doc/70542118/

[59] Хилюта В.В. Вопросы квалификации преступлений против собственности не являющихся хищением. Минск: «Пересвет», 2013. С. 33.

работы в указанной компьютерной программе, содержащей персональные данные клиентов ПАО «Вымпелком» и персональные данные их лицевых счетов, которые охраняются Федеральным законом «Об информации , информационных технологиях и о защите информации » № 149-ФЗ от 27 июля 2006 года умышленно из корыстной заинтересованности, используя свое служебное положение, с целью неправомерного доступа к охраняемой законом компьютерной информации , с целью ее модификации, под своими индивидуальными и учетными данными осуществила доступ в компьютерную программу «1С» и, указав кассиром Г. Д.В., неправомерно внесла сведения в товарный чек о внесении клиентом в кассу предприятия денег в сумме 16000 рублей для совершения платежа в биллинг, без фактического внесения денег в кассу, тем самым модифицировала компьютерную информацию.[60]

М. И. Третьяк, высказывает свою позицию, согласно которой существенным признаком совершения мошенничества путем модификации компьютерной информации является то, что у виновного лица имеется законный доступ к компьютерной информации. Я считаю, что данная позиция является спорной, так как факт обладания лицом права на доступ к компьютерной информации никак не влияет на суть самого деяния.

Диспозиция нормы мошенничества в сфере компьютерной информации содержит открытый перечень способов хищения. Так, к способам совершения преступления, ответственность за которое предусмотрена ст. 159.6 УК РФ, законодатель также отнес иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Подобное вмешательство описывается в литературе как осуществление неправомерных действий, нарушающих установленный процесс обработки, хранения, использования, передачи и иного реального обращения с компьютерной

[60] Приговор Октябрьского городского суда Республики Башкортостан № 1-243/2020 от 29 июля 2020 г. по делу № 1-243/2020. [Электронный ресурс] // Справочная правовая система «СудАкт». – Режим доступа: http://www.sudact.ru.

информацией.[61] В доктрине уголовного права существует два подхода к пониманию «иного вмешательства» в узком и широком смысле. В узком смысле термин «иное вмешательство» не охватывает своим содержанием способы, описанные в статьях гл. 28 УК РФ. При узкой трактовке данного термина можно говорить о совокупности ст. 159.6 УК РФ со статьями из гл. 28 УК РФ, так как они не охватываются составом мошенничества в сфере компьютерной информации. Широкое понимание данного термина указывает на то, что под «иным вмешательством» следует понимать любые способы осуществления хищения в сфере компьютерной информации, кроме тех, которые уже указаны в диспозиции ст. 159.6 УК РФ, то есть это «ввод», «удаление», «блокирование», «модификация» компьютерной информации. При трактовке в широком смысле следует говорить о том, что состав преступления, предусмотренный ст. 159.6 УК РФ, относится к составам преступлениям из главы 28 УК РФ как целое к части, из-за чего возникает конкуренция норм.

Так, согласно разъяснениям Пленума Верховного Суда РФ от 27 декабря 2007 г. N 51 «О судебной практике по делам о мошенничестве, присвоении и растрате», по смыслу ст.159.6 УК РФ, вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно- телекоммуникационных сетей признается целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) – ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно- телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной

[61] Дворецкий М.Ю. Уголовная ответственность за мошенничество в сфере компьютерной информации: проблемы теории и правоприменительной практики // Вестник ТГУ. 2013. №8 (124). С. 408.

информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него.[62]

Не рассмотренным осталось понятие «средства хранения, обработки и передачи компьютерной информации», содержащееся в ч. 1 ст. 159.6 УК РФ. По мнению большинства учёных данное понятие нуждается в уточнении и тщательной проработке. Под средствами хранения, обработки и передачи компьютерной информации следует понимать любые электронные (цифровые) устройства, способные работать с различными данными, а также электронные (машинные) носители данных. К средствам хранения компьютерной информации относятся ее материальные носители: дискеты, жесткие диски, оптические диски, USB-флешнакопители, карты памяти и др. Инструментом обработки служит компьютер, т.е. электронное устройство, предназначенное для автоматической обработки информации путем выполнения заданий, определенных последовательностью операций. Каналы связи, по которым передается компьютерная информация, могут быть проводными и беспроводными. Однако не ясно, почему законодатель использует именно термин «средства хранения, обработки и передачи компьютерной информации», вместо например «ЭВМ». Так как под средством хранения компьютерной информации можно понимать и картонную коробку и кейс, где можно хранить электронные носители компьютерной информации(диски, флеш-карты).

В связи с этим следует согласиться с мнением Ефремовой М.А., что понятие «средства хранения, обработки и передачи компьютерной информации», содержащееся в ч. 1 ст. 159.6 УК РФ, нуждается в уточнении и тщательной проработке. Широкое распространение технических устройств, обладающих процессорами и собственным программным обеспечением и интегрированным в локальные или глобальные информационные сети (сотовые телефоны, смартфоны, платежные терминалы, контрольно-кассовые

[62] 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.

машины), порождает проблемы отнесения указанных устройств к «средствам хранения, обработки и передачи компьютерной информации» и, соответственно, квалификации преступных действий, совершенных с их использованием.[63]

О месте совершения компьютерного мошенничества правильно заключает В.В. Коломинов: «Рассматривая характерные особенности функционирования компьютерной сети, можно сделать вы воды о том, что, с одной стороны, местом совершения мошенничества в сфере компьютерной информации является сама информационно-телекоммуникационная сеть, в которой происходит ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации. С другой стороны, местом совершения мошенничества в сфере компьютерной информации является местонахождение конкретного компьютера, с которого осуществляется не правомерный доступ». В.В. Коломинов относит к месту совершения преступления также компьютерно-технические средства потерпевшего.[64]

Рассмотрев особенности объективной стороны мошенничества в сфере компьютерно инфорамации можно выделить ряд особенностей и специфических черт. Во-первых воздействие осуществляется непосредственно на компьютерную информацию, а не на сознание потерпевшего; во-вторых, отсутствует обман, обязательным признаком которого является введение другого лица в заблуждение путем воздействия на сознание (психику) другого человека; в-третьих, отсутствует передача имущества или приобретение права на имущество с помощью потерпевшего; в-четвертых, орудием преступления признаются информация, средства хранения, передачи и обработки компьютерной информации, а не ложные

[63] Ефремова М.А. Мошенничество с использованием электронной информации // Информационное право. 2013. №4. С. 92.
[64] Коломинов В.В. Мошенничество в сфере компьютерной информации как объект криминалистического познания // Сибирские уголовно-процессуальные и криминалистические чтения. 2015. № 2 (8). С. 157.

сведения, передаваемые человеком. Изучив различные подходы к пониманию способов совершения компьютерного мошенничества, а также судебной практики, можно сделать вывод о том, что присутствует необходимость закрепления вышеупомянутых способов в Постановлении Пленума Верховного Суда, только тогда можно будет достигнуть единообразия судебной практики, так как в настоящий момент судам приходится оценивать способы

## 2.3 Субъект и субъективная сторона мошенничества в сфере компьютерной информации

Характеристика субъективных признаков мошенничества в сфере компьютерной информации предполагает последовательное рассмотрение признаков субъекта и субъективной стороны преступления, предусмотренного ст. 159.6 УК РФ.

Традиционно в уголовно-правовой теории считается, что субъектом преступления признается физическое вменяемое лицо, достигшее установленного уголовным законом возраста.[65]

В общем учении о составе преступления субъект преступления характеризуется тремя обязательными признаками. В качестве субъекта преступления может выступать только лицо: 1) физическое, 2) вменяемое и 3) достигшее возраста, с которым уголовный закон связывает возможность наступления ответственности за конкретный вид преступления. Отсутствие какого-либо из перечисленных признаков исключает наличие субъекта преступления и соответственно состава преступления.

К числу факультативных относятся признаки, характеризующие различные индивидуальные свойства лица: его гражданский, социальный или профессиональный статус; естественные демографические признаки – пол,

[65] Орлов В.С. Субъект преступления по советскому уголовному праву. М.: «Госюриздат», 1958. С. 211.

возраст; состояние здоровья; юридически значимые отношения с потерпевшим и др.

Субъект преступления, предусмотренного ст. 159.6 УК РФ общий, а именно вменяемое физическое лицо, достигшее к моменту совершения преступления возраста 16 лет.

В уголовно-правовой доктрине отсутствуют особые споры об определении субъекта мошенничества в сфере компьютерной информации. Единственный момент относительного которого у ученых расходится мнение, это возраст субъекта. Так, С. С. Медведев считает: «Возраст наступления уголовной ответственности за мошенничество необходимо понизить до 14 лет. Это связано с тем, что процесс социализации в современно обществе значительно ускорен, и, кроме этого, субъекту мошенничества в сфере высоких технологий нет необходимости иметь визуальный контакт с потенциальной жертвой».[66]

На мой взгляд, данная позиция является спорной, так как одним из характерных признаков компьютерного мошенничества является высокий уровень образования и интеллекта личности преступника. Также, распространение уголовной ответственности на более широкий круг несовершеннолетних может повлечь негативные социальные последствия, и, как представляется, вряд ли будет способствовать повышению эффективности борьбы с преступностью.

Субъективная сторона преступления – это психическая деятельность лица**,** непосредственно связанная с совершением преступления, т.е. с выполнением его объективной стороны. Она не поддается непосредственному чувственному восприятию, поэтому в практической деятельности устанавливается путем анализа и оценки всех объективных обстоятельств совершения преступления.[67] Субъективная сторона

[66] Медведев С.С. Мошенничество в сфере высоких технологий: автореф. дис. ... канд. юрид. наук. Краснодар, 2008. С. 15.
[67] Уголовное право. Общая часть: учебник / под ред. А.Н. Тарбагаева. М.: «Проспект», 2012. С. 157.

преступления включает в себя такие элементы, как вина, мотив, цель и эмоции.

Согласно действующему уголовному законодательству, вина может выступать в одной из двух форм: в форме умысла или в форме неосторожности (ст. 25 и 26 УК).

По вопросу субъективной стороны мошенничества в сфере компьютерной информации в юридической литературе практически нет противоречий, большое количество авторов считают, что преступление, предусмотренное ст. 159.6 УК РФ, совершается исключительно с прямым умыслом.

Некоторые авторы все же признают возможность совершения общественно опасного деяния как с прямым, так и с косвенным умыслом. Так, по мнению М. Ю. Дворецкого, общественно опасное деяние, предусмотренное ст. 159.6 УК РФ, относится к категории умышленных и, следовательно, может быть совершено как с прямым или косвенным умыслом.[68]

Данная позиция не представляется мне верной, поскольку мошенничество в сфере компьютерной информации, по смыслу статьи 159.6 УК РФ, есть вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Вмешательством же признается целенаправленное воздействие, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него. Следовательно, если речь идет о целенаправленном воздействии, то мы можем говорить только о прямом умысле.

[68] Дворецкий М.Ю. Уголовная ответственность за мошенничество в сфере компьютерной информации: проблемы теории и правоприменительной практики // Вестник ТГУ. 2013. №8 (124). С. 407.

По мнению В.М. Елина «виновное лицо осознаёт, что завладение чужим имуществом или правами на него производится путем ввода, удаления, блокирования, модификации компьютерной информации либо иным вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей».[69] Однако вышеуказанные условия могут не обязательно означать наличие признаков состава мошенничества в области компьютерной информации. Каждый особый случай должен объективно определять, что лицо, совершившее действие, определенное в порядке статьи 159.6 УК РФ, заведомо намеревалось использовать полученную информацию в своих корыстных целях.

Как и любая другая форма хищения, компьютерное мошенничество предполагает наличие корыстной цели, суть которой состоит в стремлении виновного обогатиться самому или обогатить других лиц за счет чужого имущества с нарушением порядка распределения материальных благ, установленного законодательством.[70] В свою очередь это предполагает, что в волевой сфере лицо желает наступления общественно-опасных последствий в виде причинения имущественного ущерба потерпевшему. Интеллектуальный момент прямого умысла при мошенничестве в сфере компьютерной информации выражается в осознании виновным характера и степени общественной опасности данного деяния, признаков объекта преступления, альтернативных способов, с помощью которых совершается хищение.

Так, Реализуя свой преступный умысел, Сайбабталов разработал план хищения, согласно которому, он в период с 17 августа по 10 сентября 2017 года похитил денежные средства ООО «Екатеринбург-2000» при следующих обстоятельствах. 17.08.2017 года в период с 11 часов 45 минут до 18 часов 12

[69] Елин В.М. Мошенничество в сфере компьютерной информации как новый состав преступления // Бизнес-информатика. 2013. №2 (24). С. 74.
[70] Гаухман Л.Д. Квалификация преступлений: закон, теория, практика. 3-е изд., перераб и дополн. М.: «ЮрИнфоР», 2005. С. 360.

минут, находясь в офисе продаж и обслуживания по адресу: ..., Сайбабталов совершил несанкционированный вход в автоматизированное программное обеспечение ООО «Екатеринбург-2000» под индивидуальной учётной записью и паролем не осведомлённой о его преступных намерениях сотрудницы ООО «"КП" зарегистрировал учётные записи нескольких абонентских номеров на вымышленные биографические данные абонентов, после чего в программе личного интернет-сервиса абонента, предоставляющей право дистанционно распоряжаться денежными средствами на лицевом счёте, осуществил операции по перечислению 250 рублей с каждого из номеров на общую сумму 5000 рублей на лицевой счёт абонентского номера, подконтрольный ему, получив таким образом возможность распоряжаться денежными средствами в общей сумме 5000 рублей по своему усмотрению.

Следовательно, Сайбабталов зарегистрировал учетные записи вымышленных абонентов с целью перевести на свой счет определенную сумму денежных средств, и воспользоваться ей.

Дискуссионным считается вопрос о возможности признания корыстной цели в случаях, когда виновный стремился не к личному обогащению или обогащению своих близких, а других лиц, в том числе лично с ним незнакомых.

В соответствии с п. 26 постановления Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» при решении вопроса о виновности лиц в совершении мошенничества, присвоения или растраты суды должны иметь в виду, что обязательным признаком хищения является наличие у лица корыстной цели, то есть стремления 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 ограничен.[71]

С. А. Петров отмечает, что под корыстной целью следовало бы понимать стремление виновного противоправным путем получить реальную возможность владеть, пользоваться и распоряжаться чужим имуществом как своим собственным, а равно незаконно извлечь иные выгоды имущественного характера не только для себя, но и для других лиц, в том числе посторонних для виновного.

Я считаю, что желание лица увеличить имущественную массу незнакомого человека независимо от имевшей место мотивации (сострадание, бравирование, месть или зависть по отношению к потерпевшему), не исключает присутствия корыстной цели. Хотя это и весьма нетипично для хищения, но корыстная цель может и не предполагать личного отношения виновного с лицом, в пользу которого отчуждается имущество.

Так, например, в случае если лицо хочет стать частью преступного сообщества, и члены данного сообщества дают этому лицу «задание» совершить компьютерное мошенничество. Похищенные средства не переходят в пользование лица, а являются подтверждением успешно выполненного задания. В данном случае корыстная цель все равно не исключается.

[71] 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.

## Глава 3. Отграничение мошенничества в сфере компьютерной информации от смежных составов

С момента введения нормы о компьютерном мошенничестве и до сегодняшнего дня существует достаточно много проблем по поводу отграничения данного вида преступлений от смежных по составу, что находит свое отражение в судебной практике.

Проанализировав во второй главе основные элементы состава преступления, предусмотренного ст.159.6 УК РФ, можно сделать вывод, что схожими чертами мошенничества в сфере компьютерной информации с составом кражи является объект посягательства – им выступают отношения собственности. Тем не менее, определение объекта преступления, предусмотренного ст. 159.6 УК РФ является более обширным, так как

посягает также и на дополнительный объект, а именно отношения в сфере компьютерной информации.

Кроме того, данные два вида преступлений имеют сходство относительно наступления общественно-опасных последствий вследствие их совершения. Необходимо упомянуть, что в данных составах существует различие в способе совершения преступления. Это проявляется в том, что при краже преступник, для завладения вещью оказывает на нее непосредственное физическое воздействие, что отсутствует при совершении мошенничества в сфере компьютерной информации, так как оно совершается исключительно путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно телекоммуникационных сетей, при этом непосредственного воздействия на человека не осуществляется. Различия между составами преступлений состоит и в субъекте, которым в силу ст. 20 УК РФ, согласно статье 158 УК РФ, может быть физическое вменяемое лицо, достигшее возраста 14 лет, а в соответствии со ст. 159.6 УК РФ – 16 лет.

Более того, в отграничении данных двух видов преступлений важно обратить внимание на следующий момент, на который обращает внимание Верховный суд Российской Федерации в соответствии с пунктом 21 Постановления Пленума Верховного суда Российской Федерации от 30 ноября 2017 года №48 «О судебной практике по делам о мошенничестве, присвоении и растрате». Данный пункт гласит, что в случае совершения хищения имущества и приобретения прав на него путем использования учетных данных собственника или иного владельца имущества независимо от применяемого способа получения доступа к таким данным, если виновным не было оказано незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-

телекоммуникационные сети, то такие действия должны квалифицироваться как кража.[72]

В качестве примера можно привести приговор Димитровградского городского суда Ульяновской области от 22.08.2017 С.Ю.А., в котором С.Ю.А. был признан виновным в совершении преступлений, предусмотренных ч.1 ст. 159.6 УК РФ и ч.1 ст. 161 УК РФ. С.Ю.А. в целях незаконного завладения чужими денежными средствами, воспользовался похищенным планшетом, в частности сим-картой, которая являлась непосредственной его частью и которая была подключена к услуге «Мобильный банк». С.Ю.А. совершил с ее помощью отправку смс сообщений на номер «900» с целью перевода денежных средств на номер телефона, к которому у него был доступ. В результате со счета банковской карты потерпевшей произошло списание денежных средств.[73]

Суд, вменяя состав преступления, предусмотренного ст.159.6 УК РФ, учел, что отправка смс-сообщений на соответствующий номер, представляла собой ввод компьютерной информации в форме сигнала, что являлось способом совершения мошеннических действий и, следовательно, образовывало состав мошенничества в сфере компьютерной информации.

Однако похожая ситуация была квалифицирована судом совсем иначе. Так, в приговоре от 22.12.2016 по делу 1 274/2016, Володарским районным судом г. Брянска. П.М.Ю. с целью похищения чужих денежных средств с использованием смс-сообщений на номер «900» перевел денежные средства с банковского счета потерпевшего на номер телефона, к которому у него был доступ. Суд, рассмотрев материалы дела, вменил подсудимому п. «в» ч.2 ст.

[72] 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.

[73] Приговор Димитровградского городского суда Ульяновской области [Электронный ресурс] : приговор от 22.08.2017 по делу № 1-256/2017 // Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). - Режим доступа: https://sudact.ru/

158 УК РФ, то есть хищение денежных средств с причинением ущерба гражданину значительной степени.[74]

Кроме того, абсолютно верно замечает Р.Ю. Шергин: «Поставив во главу угла факт противоправного воздействия на компьютерную информацию, технически используемую для обеспечения сохранности или учета имущества, мы рискуем перевести в сферу применения ст. 159.6 УК любые другие формы хищений, а именно кражи, некоторые виды присвоений и растрат, при простом применении в ходе их совершения компьютерного устройства для решения каких-либо второстепенных преступных задач: взлом цифрового замка хранилища, отключение его сигнализации, отправка бухгалтерских или иных документов на вверенное имущество по электронной почте и т.п.».[75]

Исходя из этого, можно сделать вывод, что в российском законодательстве существуют правовые разногласия в отношении классификации данных видов преступлений. Несмотря на то, что в Постановлении Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» существует достаточно ясная формулировка относительно случаев применения статей 159.6 и 158 УК РФ соответственно, суды все же испытывают затруднения относительно применения данных норм, так как ст. 159.6 УК РФ и случаи ее применения недостаточно полно представлены.

Отграничивая рассматриваемый вид преступления от мошенничества с использованием средств электронного платежа (ст.159.3 УК РФ), необходимо обозначить объекты и субъекты данных преступлений для сравнения. Субъекты этих преступлений одинаковы, а именно физическое лицо, достигшее 16 лет, субъективная же сторона охарактеризована умышленной формой вины, то есть субъект, согласно ст. 159.3 и 159.6 УК РФ

[74] Приговор Володарского районного суда г. Брянска [Электронный ресурс] : приговор от 22.12.2016 по делу № 1-274/2016 // Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). – Режим доступа: https://sudact.ru/

[75] Шергин Р.Ю. Уголовная ответственность за компьютерное мошенничество: новое не всегда лучшее // Законность. 2017. № 5. С.45.

понимает общественную опасность своих деяний и предвидит возможность наступления общественно-опасных последствий.

Объектом преступления согласно ст. 159.3 «Мошенничество с использованием электронных средств платежа» УК РФ являются отношения собственности, точно такой же основной объект у преступления, предусмотренного ст. 159.6 УК РФ. Данные нормы входят в главу 21 УК РФ «Преступления против собственности» и являются специальными по отношению к общей статье о мошенничестве, закрепленной в ст. 159 УК РФ.

Однако, между данными нормами существует ряд различий. В первую очередь это касается объективной стороны. Можно определить объективную сторону мошенничества с использованием средств электронного платежа как хищение чужого имущества, которое совершается с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем обмана уполномоченного работника кредитной, торговой или иной организации.

Рассматривая подробнее составы статей 159.3 и 159.6 УК РФ можно сделать вывод, что несмотря на то, что оба состава являются разновидностью мошенничества, что должно являться их схожим аспектом, отличаются по формулировке объективной стороны. В статье 159.6 УК РФ мошенничество в сфере компьютерной информации, как уже было упомянуто во второй главе[76] не включает в себя такой признак объективной стороны, как обман и злоупотребление доверием, что, безусловно, является одним из важнейших признаков мошенничества. Рассматривая сам факт обмана в качестве способа совершения мошенничества, можно с уверенностью сказать, что последний может быть целесообразен только в межличностных отношениях. Действительно, статья 159 УК РФ и Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о

[76] Пояснительная записка к законопроекту № 53700-6 «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» // Система обеспечения законодательной деятельности [сайт]. – Режим доступа: https://sozd.duma.gov.ru.

мошенничестве, присвоении и растрате» [77] трактует нам факт мошенничества как ни что иное как хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. Рассматривая же статью 159.6, которая стоит особняком в главе о мошенничестве, можно определить, что обман как признак объективной стороны мошенничества в сфере компьютерной информации в диспозиции данной статьи в отличие от статьи 159.3 УК РФ, прямо не оговорен и не вытекает из ее содержания компьютерного мошенничества.

Подтвердить факт отсутствия обмана при совершении мошенничества в сфере компьютерной информации можно исходя из содержания п.1 Постановления Пленума Верховного суда Российской Федерации от 30 ноября 2017 года №48 «О судебной практике по делам о мошенничестве, присвоении и растрате». Кроме того, в данном Постановлении исходя из вышеуказанного пункта, можно сделать вывод, что преступления, предусмотренные ст. 159.6 совершаются не путем обмана или злоупотребления доверием.[78]

По мнению Е.И. Майоровой проблема разграничения данных норм в том, что объективная сторона составов данных преступлений имеют много схожего, однако они не идентичны. В ст. 159.3 УК РФ хищение происходит с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты, путем обмана уполномоченного работника кредитной, торговой или иной организации. Здесь прослеживается тот факт, что средства совершения данного преступления совпадают со ст. 159.6 УК РФ - ими являются платежная карта и иные средства хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационные сети. При этом законодатель в конструкции

[77] 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.

[78] Иванов М.Г., Николаев А.Ю. Проблемы разграничения составов имущественных преступлений, связанных с информационными технологиями (ст. 159.3, 159.6 и п. «г» ч. 3 ст. 158 УК РФ) // Вестник Российского университета кооперации. 2020. №3 (41). С. 124.

диспозиции ч. 1 ст. 159.3 УК РФ применяет термин «использование», подразумевающий под собой абсолютно любой способ совершения данного преступления, в том числе ввод компьютерной информации и иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Для наглядной иллюстрации различия данных составов можно использовать следующие примеры: так, по мнению Мусьял «если лицо, используя специальное вредоносное программное обеспечение на компьютере потерпевшего, получило доступ к банковской системе, с помощью которого потерпевший осуществлял переводы денежных средств с банковского счета, и осуществило хищение имущества, то данное преступление следует квалифицировать по ст. 159.6 УК РФ, за неимением взаимодействия непосредственно с потерпевшим, а следовательно неимением в составе преступления обмана в качестве способа совершения преступления». Все же по ст. 159.3 УК РФ преступление может быть квалифицировано если же лицо с помощью вредоносного программного обеспечения получило информационные данные о карте клиента на собственное мобильное устройство для последующего проведения оплаты с помощью использования мобильного приложения, и впоследствии осуществило покупку в магазине. Тем самым, произошло хищение денежных средств. В данной ситуации, способом совершения преступления являлся именно обман уполномоченного работника торговой организации, в то время как внедрение программ обеспечения было лишь способом доступа собственности потерпевшего.[79]

Таким образом, можно с уверенностью сказать, что обман, в качестве необходимой составляющей действительно не предусматривается в качестве признака объективной стороны преступления, предусмотренного ст. 159.6

[79] Мусьял И.А. Мошенничество с использованием платежных карт // Проблемы правоохранительной деятельности. 2017. №1. С. 25.

УК РФ, отсюда следует, что мошенничество в сфере компьютерной информации не является видом мошенничества в традиционном понимании этого понятия. Исходя из этого, многие исследователи высказывают точку зрения относительно того, что данный вид преступлений представляет собой совершенно новую форму хищения. Данное заявление достаточно обосновано по моему мнению, так как в действительности, как уже было сказано во второй главе, создание данной нормы из-за отличительных особенностей ее диспозиции от привычных норм о мошенничестве принципиально разнится и соответственно составляет целый пласт сложностей для правоприменения.

Сравнивая преступления, предусмотренные ст. 159.6 и 272 «Неправомерный доступ к компьютерной информации» УК РФ, необходимо в первую очередь обозначить объект преступлений. Объектом ст.272 УК РФ являются отношения в сфере безопасности компьютерной информации, рассматривая подробнее объект данного вида преступления можно дополнить данное пояснение отношениями, связанными с обеспечением безопасности конкретного вида информации, таких как, государственная тайна, коммерческая тайна, банковская тайна, и т.п., а также общественными отношениями, обеспечивающими информационную безопасность конкретного субъекта. Кроме того, расширяется и объективная сторона данного вида преступления, которая заключается в неправомерном доступе к охраняемой законом информации, хранящейся в электронно-вычислительных машинах. По мнению Шевелевой, способы совершения такого рода преступлений согласно статьям 159.6 и 272 УК РФ достаточно схожи, так как информационное поле дает огромное количество возможностей преступникам. Способы совершения таких действий достаточно разнообразны. Субъектом преступления согласно ст. 272 УК РФ физическое вменяемое лицо, достигшее возраста 16-ти лет, субъективная сторона вина в форме умысла, но как прямого, так и косвенного, что и составляет различие между двумя видами преступления, так как согласно ст.

159.6 УК РФ субъективная сторона, как было отмечено ранее принимает только форму прямого умысла. Рассматривая же неправомерный доступ к компьютерной информации, прямой умысел означает желание и допущение лицом, которое совершило преступление, наступления последствий, а косвенный умысел означает отсутствие четкого намерения о наступлении тех последствий, которые перечислены в комментируемой статье.

Важнейшее отличие двух видов преступления это материальный состав, который предусматривает ст. 272 УК РФ. Для того чтобы преступление считалось оконченным должно наступить по крайней мере одно из следующих последствий, а именно 1) уничтожение информации, то есть прекращение факта ее существования, при невозможности ее восстановления; 2) блокирование информации - невозможность доступа к информации, то есть отсутствие возможности сбора, обработки, пользования, хранения и совершения иных действий в отношении информации; 3) модификацию информации - любое изменение относительно информационных данных, такое как, искажение исходных данных, добавление нового содержания информации, частичное уничтожение исходной информации; 4) копирование информации - создание аналога информации на материальных носителях путем перенесения данных от исходной информации, но с сохранением ее первоначального содержания.

Отсутствие системности в действиях законодателя привело к тому, что ст. 159.6, являющаяся специальной по отношению к ст. 159, конкурирует по основному составу с основными составами ч.1 с. 272 и ч.1ст. 273 УК РФ.

В литературе по этому вопросу высказываются достаточно категоричные формулировки. Так, по мнению З.И. Хисамовой статья 159.6 УК РФ является специальной по отношению к статьям 272, 273 УК РФ. Суть рассуждений заключается в том, что неправомерный доступ к компьютерной информации из корыстной заинтересованности является действием, направленным на хищение, следовательно, компьютерная информация выступает средством доступа к чужому имуществу, что входит в

объективную сторону статьи 159.6 УК РФ. В силу требований части 3 статьи 17 УК РФ дополнительной квалификации по статьям 272, 273 УК РФ не требуется.

Следует учитывать то обстоятельство, что способы совершения компьютерного мошенничества лишь отчасти перекликаются с указанными в диспозиции статьи 272 УК РФ способами. Законодатель использует термин «иное вмешательство» в статье 159.6 УК РФ, что позволяет утверждать, что способов совершения компьютерного мошенничества больше.

Кроме того, при совершении мошенничества в сфере компьютерной информации доступ к этой информации может носить как законный, так и незаконный характер, тогда как в статье 272 УК РФ речь идет о неправомерном доступе к охраняемой законом компьютерной информации.

По мнению Шевелевой «необходимо учитывать, что состав преступления, предусмотренный статьей 159.6 УК РФ, относится к числу сложных преступлений, которые могут совершаться посредством других преступлений-способов, необходимо выработать общий подход к правилам квалификации в подобных случаях. В.Н. Кудрявцев справедливо отмечал, что, если способ совершения преступления является самостоятельным преступлением, его вменение по совокупности с основным преступлением не требуется. Н.Ф. Кузнецова, придерживаясь аналогичной позиции, добавляла, что преступление-способ не может вменяться только в том случае, если по тяжести он ниже основного состава преступления. В случае если тяжесть преступления-способа совпадает с основным преступлением, а тем более если выше, то требуется дополнительная квалификация. Кроме того, по мнению Н.Ф. Кузнецовой, еще одним условием отсутствия совокупности преступлений должно быть единство объекта. Относительно квалификации статьи 272 УК РФ с иными составами преступлений, где неправомерный доступ является преступлением-способом, Н.Ф. Кузнецова указывала на необходимость определения вида совокупности: при реальной совокупности должна быть квалификация и по статье 272 и по основному составу, при

идеальной совокупности оценка преступных действий дается только по основному составу, то есть в нашем случае только по статье 159.6 УК РФ».[80]

Кроме того, учитывая то, что характер использования при совершении хищений информационно-коммуникационных технологий в целом и электронных средств платежа в частности, некоторые исследователи считают разумным использовать при квалификации рассматриваемых посягательств расширенное толкование мошенничества в сфере компьютерной информации и квалифицировать по норме статьи 272 все случаи мошенничества в сети Интернет, совершаемые со всеми видами вмешательств для осуществления платежей. Очевидно, что деяния должны быть квалифицированы по совокупности различных составов УК РФ.

По мнению Хисамовой «отсутствие системности в действиях законодателя привело к тому, что ст. 159.6 конкурирует по основному составу (ч. 1 ст. 159.6) с основными составами ч. 1 ст. 272 УК РФ. Особенно остро это противоречие проявляется при неоконченном преступлении, когда установить умысел на хищение чужого имущества достаточно сложно. конкурируют между собой и квалифицирующие признаки указанных статей: неправомерный доступ к охраняемой законом компьютерной информации, повлекший указанные в законе последствия, причинивший крупный ущерб и совершенный из корыстной заинтересованности, идентичен по содержанию мошенничеству в сфере компьютерной информации, совершенному в крупном размере. По мнению исследователя, ст. 159.6 является специальной по отношению к ст. 272 УК РФ, так как неправомерный доступ к компьютерной информации из корыстной заинтересованности представляет собой действия, направленные на хищение, то есть компьютерная информация выступает средством доступа к чужому имуществу, что охватывается объективной стороной ст. 159.6 УК РФ, в связи с чем

[80] Шевелева С.В. Мошенничество в сфере компьютерной информации: особенности квалификации и конкуренции со смежными составами преступлений // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2017. №4 (40). С. 229.

дополнительной квалификации ст. 272 УК РФ мошеннических действий в данной сфере не требуется».[81]

Однако я не согласна с данной точкой зрения и считаю, что данные статьи, а именно ст. 159.6 и ст. 272 УК РФ необходимо применять в совокупности, так как следует учесть то, что способы совершения компьютерного мошенничества по ст. 159.6 лишь отчасти перекликаются с указанными в диспозиции статьи 272 УК РФ способами. Законодатель использует термин «иное вмешательство» в статье 159.6 УК РФ, что позволяет полагать, что способов совершения компьютерного мошенничества предусмотрено больше. [82]

Рассмотрев некоторые моменты, по которым данные два вида преступлений схожи и увидев уровень сложности способа их разграничения, можно сделать вывод, что состав преступления, предусмотренный статьей 159.6 УК РФ, относится к числу сложных преступлений, понятие которых включает в себя возможность их совершения посредством других преступлений.

В.Н. Кудрявцев в своей статье отмечал, что, в случае признания способа совершения преступления, не частью, а самостоятельным преступлением, его вменение по совокупности с основным преступлением не требуется.[83] Однако существует и друга точка зрения исследователей.

Например, Н.Ф. Кузнецова, придерживаясь схожей позиции, определяла, что преступление-способ не может вменяться только в случае, если по тяжести он ниже основного состава преступления. [84]

---

[81] Хисамова З. И. Квалификация посягательств, совершенных с использованием электронных средств платежа // Юридическая наука и правоохранительная практика. 2015. № 3(33). С. 127.

[82] Шевелева С.В. Мошенничество в сфере компьютерной информации: особенности квалификации и конкуренции со смежными составами преступлений // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2017. С. 230.

[83] Кудрявцев В.Л. Преступления в сфере компьютерной информации: общая характеристика // Уголовное законодательство в XXI веке. 2013. №2. С. 69.

[84] Кузнецова Н.Ф. Проблемы квалификации преступлений: лекции по спецкурсу «Основы квалификации преступлений» / науч. ред. и предисл. В.Н. Кудрявцева. М., 2007.

Если же складывается ситуация, что тяжесть преступления-способа совпадает с основным преступление или выше, то требуется дополнительная квалификация.

Приведенные правила квалификации были применены в судебной практике. Так, Б.Н., Б.С., С.В. путем установки в Белгороде на банкоматы ОАО «Сбербанк России» устройства, предназначенного для негласного получения информации, намеревались совершить хищение денежных средств со счетов клиентов банков. Участники данного преступления предполагали считать электронную информацию с карты памяти неизвестного устройства, крепившегося ими на банкоматы, и далее передать ее изготовителю поддельных карт, но в силу того, что они были задержаны сотрудниками полиции, довести свой преступный умысел до конца им не удалось. Все подсудимые были признаны виновными в совершении преступлений, предусмотренных частью 2 статьи 35, частью 3 статьи 183; частью 3 статьи 30, частью 2 статьи 159.6 УК РФ.[85]

По мнению Сухаренко, который приводит пример по уголовному делу №1-336/2017, в ходе которого промышленным районным судом г. Курска в отношении И.М.А. был вынесен обвинительный приговор, которым он был признан виновным в совершении преступлений, предусмотренных ч.3 ст. 272, ч.1 ст.159.6, ч.3 ст. 272 УК РФ. Осужденный, являясь специалистом одного из операторов сотовой связи, путем неправомерного доступа к охраняемой законом компьютерной информации перевыпустил сим-карту одного из абонентов, на счету которой находились денежные средства в сумме 11600 рублей, без согласия последнего.

В дальнейшем, используя новую сим-карту, с номером потерпевшего И.М.А. вставил ее в сотовый телефон и посредством отправки смс-сообщений перевел с абонентского номера потерпевшего на подконтрольный

[85] Приговор Свердловского районного суда г. Белгорода [Электронный ресурс] : приговор от 20.05.2018 по делу № 1-64/2018 // Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). – Режим доступа: https://sudact.ru/

ему абонентский номер денежные средства, совершив, таким образом, преступление, предусмотренное ст. 159.6 УК РФ.[86]

Рассмотрев данные сложности в отграничении двух данных видов преступления путем обозначения различных подходов к квалификации подобного рода хищений.

Я считаю, что в данном случае необходимо создать предпосылки в законодательстве к применению ст. 159.6 и 272 УК РФ. Так как представляется закономерным данное применение в части того, что информационное поле достаточно сложно поддается изучению и тем более оценке.

Исходя из вышеизложенных позиций, решение суда об отказе от обвинения по ст. 272 УК РФ было обосновано тем, что основной состав и умысел виновного лица были направлены именно на совершение хищения, а это является идеальной совокупностью, следовательно, квалифицировать данное преступление суд будет по основному составу.

Таким образом, можно прийти к выводу, что такая норма как мошенничество в сфере компьютерной информации имеет схожесть со многими смежными составами, что, безусловно, составляет трудность в правоприменительной практике. Законодатель трактует похожие составы преступления по-разному, что является причиной подачи жалоб в апелляционные суды и разногласия в законодательстве в целом.

Итак, действующая редакция статьи 159.6 УК РФ нуждается в разъяснениях Пленума Верховного Суда РФ. Учитывая сложившуюся разницу между судебной практикой и доктринальной трактовкой компьютерного мошенничества, судам следует дать разъяснения.

К таким выводам можно прийти исходя из достаточно специфичного объективного состава преступлений данного вида, а именно его двуобъектности, что и составляет сложности назначения наказания, ведь

[86] Сухаренко А.Н. Законодательное обеспечение информационной безопасности в России // Российская юстиция. 2018. № 2. С. 3.

несмотря на основной объект в виде отношений собственности, вторым не менее важным объектом преступления являются отношения в сфере безопасности компьютерной информации, что делает возможным квалификацию ст. 159.6 в совокупности со ст. 272 УК РФ.

Таким образом, с учетом изложенного, можно прийти к следующим выводам:

- деяние, предусмотренное ст. 159.6 УК РФ, является не мошенничеством в его традиционной трактовке, а новой формой хищения с использованием специфических способов совершения данного преступления, о чем говорилось при отграничении ст. 159.6 от 159.3 УК РФ;
- необходимо более широкая трактовка по совокупности части деяния и целого, в том числе, применительно к преступлениям, предусмотренным ст. 159.6 УК РФ и 272 УК РФ;
- отграничение преступления, предусмотренного ст. 159.6 УК РФ от смежных составов следует проводить по некоторым признакам, в особенности по способу совершения деяния. В случае если завладение денежными средствами произошло непосредственно в результате ввода в т.ч. посредством использования чужой электронной подписи, модификации, удаления, блокирования, то данное деяние следует квалифицировать по ст. 159.6 УК РФ.

## Заключение

Изучив нормы уголовного права зарубежных стран об ответственности за компьютерное мошенничество, можно сделать вывод о том, что большое количество государств своевременно принимают соответствующие меры для реформирования и изменения национального уголовного законодательства. Что касается компьютерного мошенничества, его единое определение

отсутствует, но общепринятой практикой является очень общее определение компьютерного мошенничества, понимаемого как действие, совершенное с использованием компьютерной информации для личной выгоды.

В законодательстве стран СНГ практически полностью отсутствует закрепление норм о мошенничестве в сфере компьютерной информации во многом связано с влиянием соглашения государств-членов СНГ о сотрудничестве в борьбе с преступлением в области компьютерной информации, где такой состав не выделялся отдельно. Однако не только Россия, но и некоторые другие страны Содружества (Армения и Белоруссия) внесли изменения в угловые кодексы с целью конкретно определить ответственность за хищение с использованием компьютерной информации.

Проанализировав норму о мошенничестве в сфере компьютерной информации, обозначив дискуссионные позиции относительно субъектного и объектного состава данного вида преступления и сравнив его со смежными составами, можно прийти к выводу о том, что существуют сложности относительно названия и содержания данной нормы. Это объяснено тем, что в составе компьютерного мошенничества отсутствует факт обмана или злоупотребления доверием, что является необходимой составляющей мошенничества, и закреплено в предыдущих пяти статьях 159.1-159.5 УК РФ, а потому позиция считать мошенничеством данный вид преступления нецелесообразна. Кроме того, мошенничество предполагает непосредственный контакт преступника с жертвой, чего также не наблюдается в составе компьютерного мошенничества.

В настоящее время ни в одном законодательном и правоприменительном акте нет определения способов совершения компьютерного мошенничества. Соответственно, считается необходимым внести изменения в п.20 Постановления Пленума Верховного Суда РФ, путем добавления новых положений, в следующем виде:

«Ввод компьютерной информации – определенный алгоритм действий по набору данных для их последующей обработки или хранения.

Удаление компьютерной информации – это приведение информации или ее части в непригодное для использования состояние независимо от возможности ее восстановления.

Блокирование компьютерной 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.

Модификация компьютерной информации – внесение в компьютерную информацию любых изменений, которые обусловят ее отличие от ранее хранившейся в компьютерной сети, системе или на машинном носителе собственника информационного ресурса».

Также, нерешенным является вопрос по поводу предмета преступления, предусмотренного данной статьей. Для формирования единообразной судебной практики я считаю необходимым внесение в вышеназванный пункт Постановления Пленума Верховного суда РФ уточнение о том, что:

«В качестве предмета компьютерного мошенничества могут выступать безналичные электронные денежные средства, новые виды цифровых финансовых активов, премиальные денежные суррогаты, возникающих в связи с реализацией разнообразных программ потребительской лояльности».

Таким образом, рассмотренный мной состав представляет собой самостоятельную форму хищения со специфичным способом, отличным от других форм хищения чужого имущества. Данными способами являются ввод, удаление, блокирование, модификация компьютерной информации, иное вмешательство в функционирование средств хранения, обработки или

передачи компьютерной информации или информационно-телекоммуникационных сетей. Следовательно, название и диспозиция данной нормы нуждаются в изменении и доработке.

Уголовно-правовую норму о мошенничестве в сфере компьютерной информации предлагается изложить в следующей редакции:

«Статья 159.6 Хищение, совершенное с использованием информационно- телекоммуникационных технологий.

1. Хищение чужого имущества или приобретение права на чужое имущество, совершенное посредством ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, - наказывается …»

## Список использованных источников

### I. Нормативные правовые акты

1. Уголовный кодекс Российской Федерации. [Электронный ресурс] : федер. закон от 13.06.1996 № 63-ФЗ ред. от 31.07.2020 // Справочная

правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

2. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации. [Электронный ресурс] : федер. закон от 29.11.2012 № 207-ФЗ ред. от 03.07.2016 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

3. Об информации, информационных технологиях и о защите информации [Электронный ресурс] : федер. закон от 27.07.2006 № 149-ФЗ ред. от 08.06.2020 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

4. Уголовный кодекс Республики Беларусь [Электронный ресурс] - Режим доступа: https://kodeksy-by.com/ugolovnyj_kodeks_rb.htm.

5. Уголовный кодекс Германии. [Электронный ресурс]. – Режим доступа: URL: http://www.gesetze-im-internet.de/englisch_stgb/ englisch_stgb. html#p2344.

6. Уголовный кодекс Испании. [Электронный ресурс]. – Режим доступа: URL: http://legislationline.org/documents/section/criminal-codes.

7. Уголовный кодекс Республики Казахстан / Закон Республики Казахстан от 16 июля 1997 года № 167 (Ведомости Парламента РК, 1997 г., № 15-16, ст. 211) / Предисловие министра юстиции Республики Казахстан, докт. юрид. наук, проф. И.И. Рогова. СПб.: Изд-во «Юридический центр Пресс», 2001. 466 с.

8. Уголовный кодекс Республики Польша. [Электронный ресурс]. – Режим доступа: URL:http://www.polskieustawy.com.

9. Свод законов США. [Электронный ресурс]. – Режим доступа: http://law.justia.com/codes/us/2012/title-18/part-i/chapter-47/section-1030.

10. Уголовный кодекс Финляндии. [Электронный ресурс]. – Режим доступа: URL: http://legislationline.org/documents/section/criminal-codes.

11. Уголовный кодекс Швеции. [Электронный ресурс]. – Режим доступа: URL: http://legislationline.org/documents/section/criminal-codes.

## II. Судебная практика

12. 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.

13. Приговор Ленинского районного суда г. Владимира [Электронный ресурс] : приговор от 08.03.2013 по делу № 1-78/2013 // Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). – Режим доступа: https://sudact.ru/

14. Приговор Салаватского городского суда Республики Башкортостан [Электронный ресурс] : приговор от 21.05.2015 по делу № 1-113/2015 // Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). – Режим доступа: https://sudact.ru/

15. Приговор Володарского районного суда г. Брянска [Электронный ресурс] : приговор от 22.12.2016 по делу № 1-274/2016 // Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). – Режим доступа: https://sudact.ru/

16. Приговор Димитровградского городского суда Ульяновской области [Электронный ресурс] : приговор от 22.08.2017 по делу № 1-256/2017 // Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). - Режим доступа: https://sudact.ru/

17. Приговор Свердловского районного суда г. Белгорода [Электронный ресурс] : приговор от 20.05.2018 по делу № 1-64/2018 // Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). – Режим доступа: https://sudact.ru/

18. Приговор Свердловского районного суда города Белгорода. [Электронный ресурс] : приговор от 20.12.2019 по делу № 1-64/2019 //

Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). – Режим доступа: https://sudact.ru/

19. Приговор Октябрьского городского суда Республики Башкортостан [Электронный ресурс] : приговор от 29.10.2020 по делу № 1-243/2020 // Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). – Режим доступа: https://sudact.ru/

## III. Специальная литература.

20. Барчуков, В.К. К проблеме определения родового и видового объекта состава преступления, предусмотренного ст. 159.6 УК РФ / В.К. Барчуков // Пробелы в российском законодательстве. – 2016. – №7. – С. 160-162.

21. Барчуков, В.К. Непосредственный объект мошенничества в сфере компьютерной информации / В.К. Барчуков // Пробелы в российском законодательстве. – 2018. – №7. – С. 259-261.

22. Борисов, Е.Ф. Экономическая теория: Учебник. 3-е изд., перераб. и доп. – М.: «Юрайт», – 2005. – 399 с.

23. Беляев, Н.А. Курс советского уголовного права. Часть общая / под ред. Н. А. Беляева, М. Д. Шаргородского. – Л.: «Изд-во Ленингр. ун-та», 1968. – 648 с.

24. Бриллиантов, А.В. Уголовное право России. Части Общая и Особенная: учеб./ под ред. А.В. Бриллиантова. – М.: «Проспект», 2010. – 200 с.

25. Бушуева, Т.А., Дагель, П.С. Объект уголовно-правовой охраны природы / Т.А. Бушуева. П.С. Дагель // Советское государство и право. – М.: «Наука», – 1977, – № 8. – С. 77-84.

26. Волеводз, А.Г. Уголовное законодательство об ответственности за компьютерные преступления: опыт разных стран / А.Г. Волеводз // Правовые вопросы связи. – 2004. – № 1. – С. 37-48.

27. Гриб, Д.В. Хищение имущества путем использования информационных технологий в Уголовном кодексе Российской Федерации и Республики Беларусь: сравнительный аспект / Д.В. Гриб // Вестник Московского университета МВД России. – 2019 – № 4. – С. 75-80.

28. Гладких, В.И. Компьютерное мошенничество: а были ли основания его криминализации? / В.И. Гладких // Российский следователь. – 2014. – № 22. – С. 25-31.

29. Дворецкий, М. Ю. Уголовная ответственность за мошенничество в сфере компьютерной информации: проблемы теории и правоприменительной практики / М.Ю. Дворецкий // Вестник ТГУ. – 2013. – N 8 (124). – С. 407-410.

30. Иванов, М.Г., Николаев, А.Ю. Проблемы разграничения составов имущественных преступлений, связанных с информационными технологиями (ст. 159.3, 159.6 и п. «г» ч. 3 ст. 158 УК РФ) / М.Г. Иванов, А.Ю. Николаев // Вестник Российского университета кооперации. – 2020. – С. 123-125.

31. Коломинов, В.В. Мошенничество в сфере компьютерной информации как объект кри миналистического познания / В.В. Коломинов // Сибирские уголовно-процессуальные и криминалистические чтения. – 2015. – № 2 (8). – С. 153-160.

32. Кочои, С.М Нормы о мошенничестве в УК РФ: особенности и отличия / С.М. Кочои // Всероссийский криминологический журнал. – 2013. – №4. – С.103-107.

33. Кудрявцев, В.Л. Преступления в сфере компьютерной информации: общая характеристика / В.Л. Кудрявцев // Уголовное законодательство в XXI веке. – 2012. – №2. – С. 69-76.

34. Лопатина, Т.М. Проблемы уголовно-правовой защиты сфер компьютерной информации : современный взгляд на мошенничество / Т.М. Лопатина // Право и безопасность. – 2013. – №3-4 (45). – С. 93.

35. Мазуров, В.А. Компьютерные преступления: анализ уголовного законодательства США и Германии / А.В. Мазуров // Известия АлтГУ. – 2005. – №2. – С.59-61.

36. Малышева, Ю.Ю. Преступления, совершаемые путём обмана, по Уголовному кодексу России: понятие и виды / Ю.Ю. Малышева // Проблемы экономики и юридической практики. – 2011. – №3 – С. 34-37.

37. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] // Режим доступа: https://www.garant.ru/products/ipo/prime/doc/70542118.

38. Мусьял, И.А. Мошенничество с использованием платежных карт / И.А. Мусьял // Проблемы правоохранительной деятельности. – 2017. – С. 24-27.

39. Наумов, А.В. Уголовное право. Общая часть : курс лекций / А.В. Наумов – М.: «БЕК», – 1996. – 560 с.

40. Орлов, В.С. Субъект преступления по советскому уголовному праву./ В.С. Орлов // – М.: «Госюриздат», 1958. – 260 с.

41. Рассказов, Л.П. Англосаксонская правовая семья: генезис, основные черты и важнейшие источники / Л.П. Рассказов // Научный журнал КубГАУ. – 2015. – №. 105. – С.13-16.

42. Савельев, А.И. Электронная коммерция в России и за рубежом / А.И. Савельев // Образование и право. – 2016. – №2 – С. 40-43.

43. Саидов, А.Х. Сравнительное правоведение (основные правовые системы современности) : учебник / под ред. В. А. Туманова. – М.: «Юристъ», 2003. – С. 140-150.

44. Сафонов, О.М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: дис. ... канд. юрид. наук: 12.00.08 / Сафонов Олег Михайлович. – Москва, 2015. – 222 с.

45. Слепова, Г.В. Дискуссионные подходы к поня- тию «право на имущество» в теории уголовного права / Г.В. Слепова // Вестник Калининградского юридического института МВД России. – 2011. – №2 (24). – С. 124–128.

46. Смолин, С.В. Уголовно-правовая борьба с высокотехнологичными способами и средствами совершения преступлений / С.В. Смолин // Уголовное право. – 2014. – №4. – С. 64.

47. Сухаренко, А.Н. Законодательное обеспечение информационной безопасности в России / А.Н.Сухаренко // Российская юстиция. – 2018. – № 2. – С. 3.

48. Третьяк, М.И. Проблемы квалификации новых способов мошенничества / М.И. Третьяк // Уголовное право. – 2015. – №2. – С. 96.

49. Уголовное право. Общая часть : учебник / ред. И.Я. Козаченко. – Москва : Норма, 2008. – 720 с.

50. Уголовное право Российской Федерации. Общая Часть: учебник / ред. Л.В. Иногамова – Хегай, А.И. Рарог, А.И. Чучаев. – Москва : ИНФРА-М-КОНТРАКТ, 2011. – 560 с.

51. Уголовное право. Общая часть : учебник / ред. А.Н. Тарбагаев. – Москва: Проспект, 2012. – 448 с.

52. Устинова, Т.Д. Уголовная ответственность за лжепредпринимательство / Т.Д. Устинова. – М., 2003. – С. 51– 53.

53. Фролов, М.Д. К вопросу о предмете мошенничества в сфере компьютерной информации / М.Д. Фролов // Образование и право. – 2018. – № 3. – С. 177-184.

54. Харламов, Д.Д. Уголовная ответственность за компьютерное мошенничество по УК российской Федерации и ФРГ / Д.Д. Харламов // Проблемы экономики и юридической практики. – 2015. – №4 – С. 58-61.

55. Хилюта, В.В. Вопросы квалификации преступлений против собственности не являющихся хищением: монография / В.В. Хилюта. Минск, 2013. – 250 с.

56. Хисамова, З.И. Квалификация посягательств, совершенных с использованием электронных средств платежа / З.И. Хисамова // Юридическая наука и правоохранительная практика. – 2015. – № 3(33). – С. 127-132.

57. Чечель, Г.И., Третьяк, М.И. Законодательная регламентация преступлений против собственности в сфере высоких технологий в УК Казахстана и России / Г.И. Чечель, М.И. Третьяк // Всероссийский криминологический журнал. – 2018 – № 1. – С. 55-57.

58. Шебанов, Д.В. О некоторых проблемах квалификации мошенничества в сфере компьютерной информации / Д.В. Шебанов, Л.С. Терещенко // Теория и практика общественного развития. – 2014. – № 4. – С. 240-242.

59. Шевелева, С.В. Мошенничество в сфере компьютерной информации: особенности квалификации и конкуренции со смежными составами преступлений/ С.В. Шевелева // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2017. – С. 229- 233

60. Шумихин, В.Г. Седьмая форма хищения чужого имущества / В.Г. Шумихин // Вестник Пермского университета. – № 2 (24). – 2014. – С. 229-233.

61. Экономика: учебник / под ред. доц. А.С. Булатова. – М.: «Бек», – 1995. – 511 с.

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

Юридический
институт
Уголовного права
кафедра

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

# БАКАЛАВРСКАЯ РАБОТА

40.03.01 - Юриспруденция
код – наименование направления

Уголовно-правовая характеристика преступления, предусмотренного ч.1 ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации»

тема

Руководитель 09.06.2021 к.ю.н., доцент С.И. Бушмин
подпись, дата должность, ученая степень инициалы, фамилия

Выпускник 25.05.2021 Р.Р. Дубинникова
подпись, дата инициалы, фамилия

Красноярск 2021