Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)
Юридический институт

ДОПУСТИТЬ К ЗАЩИТЕ В ГЭК
Руководитель ООП
доктор юридических наук, профессор

_____ В.А. Уткин
подпись
«_____»_____ 2021 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА МАГИСТРА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

МОШЕНИЧЕСТВО В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: УГОЛОВНО – ПРАВОВАЯ И КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКИ

по направлению подготовки 40.04.01 Юриспруденция
направленность (профиль) «Российская уголовная юстиция»

Гапонович Кристина Витальевна

Руководитель ВКР
кандидат юридических наук, доцент

_____ А.А. Пропостин
подпись
«29» 05 2021 г.

Автор работы
студент группы № 061983

_____ К.В. Гапонович
подпись
«29» 05 2021 г.

Томск – 2021

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ЮРИДИЧЕСКИЙ ИНСТИТУТ
Магистратура

ЗАДАНИЕ
по подготовке выпускной квалификационной (магистерской) работы

студенту_____
_____
Тема
выпускной(квалификационной)работы_____
_____
_____
Утверждена_____
Руководитель
работы:_____

Сроки выполнения выпускной (квалификационной) работы:
1). Составление предварительного плана и графика написания выпускной (квалификационной) работы
с «____»_____20__г. по «____»_____20__г.

2). Подбор и изучение необходимых нормативных документов, актов и специальной литературы с «____»_____20__г. по «____»_____20__г.

3). Сбор и анализ практического материала с «____»____20__г. по «____»____20__г.
_____
_____

4). Составление окончательного плана выпускной (квалификационной) работы
с «____»_____20__г. по «____»_____20__г.

5). Написание и оформление выпускной (квалификационной) работы
с «____»_____20__г. по «____»_____20__г.

Если работа выполняется по заданию организации указать ее_____

Встречи дипломника с научным руководителем – ежемесячно (последняя неделя месяца в часы консультаций).
Научный руководитель_____

С положением о порядке организации и оформления выпускных (квалификационных) работ ознакомлен, задание принял к исполнению_____

Аннотация

магистерской диссертации

на тему: «Мошенничество в сфере компьютерной информации: уголовно-правовая и криминологическая характеристика»

В рамках данной работы была рассмотрена проблема мошенничества в сфере компьютерной информации, проведен комплексный анализ уголовно-правовой и криминологической характеристики данного преступления.

Объектом исследования являются общественные отношения, возникающие в связи с законодательным закреплением и практической реализацией уголовно-правовой нормы об ответственности за мошенничество в сфере компьютерной информации.

Предметом исследования выступает совокупность уголовных норм, научные разработки, статистические данные и судебная практика, отражающие специфику рассматриваемых правоотношений.

Целью настоящего диссертационного исследования является комплексный уголовный и криминологический анализ мошенничества в сфере компьютерной информации.

Для достижения поставленных в настоящей работе целей и задач применялись общенаучные и частно-научные методы познания.

Структура работы определена поставленными целями и задачами и включает в себя введение, две главы, содержащие шесть параграфов, заключение, список использованной литературы.

Первая глава «Уголовно-правовая характеристика мошенничества в сфере компьютерной информации», состоит из трех параграфов, посвященных анализу состава рассматриваемого преступления и отграничения его от смежных составов преступлений.

Параграф 1.1 «Объективные признаки мошенничества в сфере компьютерной информации» посвящен изучению объективных признаков анализируемого состава преступления. На основании анализа судебной

практики и научной литературы автор приходит к выводу, что анализируемый вид мошенничества специфичен по отношению к общему составу мошенничества. Хотя объектом преступления выступает, как и в общем составе мошенничества, право собственности, тем не менее преступление характеризуется специфичным способом его совершения, таким как: ввод, удаление, блокирование, модификация компьютерной информации или иное вмешательство, которое влечет за собой последствия в виде причинения ущерба субъектам права.

Параграф 1.2 «Субъективные признаки мошенничества в сфере компьютерной информации» посвящен анализу субъективных признаков анализируемого состава преступления. На основании анализа научной литературы и действующего законодательства, автор приходит к выводу, что мошенничество в сфере компьютерной информации может быть совершено как общим, так и специальным субъектом – при этом данный факт влияет на квалификацию преступления: совершение его специальным субъектом влечет более строгое наказание. Субъективная сторона характеризуется умышленной формой вины в виде прямого умысла.

Параграф 1.3 «Отграничение мошенничества в сфере компьютерной информации от смежных составов преступлений» посвящен отграничению мошенничества в сфере компьютерной информации от смежных составов преступлений. В результате проведённого анализа автор приходит к выводу, что основным преступлением, с которым смешивается мошенничество в сфере компьютерной информации, выступает неправомерный доступ к компьютерной информации. Об этом свидетельствуют и материалы судебной практики. Однако отграничивать данные посягательства между собой крайне важно – поскольку они имеют различный объект и соответственно различную степень общественной безопасности, что в конечном итоге отражается на применяемой по отношению к виновной санкции.

Глава вторая «Криминологическая характеристика мошенничества в сфере компьютерной информации», состоящая из трех параграфов

посвящена анализу показателей преступности мошенничества в сфере компьютерной информации, исследованию мер предупреждения рассматриваемого преступления и личности осужденных по ст. 159.6 УК РФ.

Параграф 2.1 «Состояние, структура и динамика мошенничества в сфере компьютерной информации» посвящен анализу основных показателей преступности в части мошенничества в сфере компьютерной информации. На основании анализа статистических данных МВД РФ и статистических данных Судебного департамента при ВС РФ, автор приходит к выводу, что состояние и структура мошенничества характеризуется сравнительным небольшим удельным весом по отношению к общему числу и отдельным видам зарегистрированных преступлений. Тем не менее автор отмечает высокую латентность рассматриваемого вида мошенничества. При этом, опираясь на статистические данные автор отмечает неутешительную динамику прироста регистрируемых преступлений анализируемого вида мошенничества.

Параграф 2.2 «Предупреждение мошенничества в сфере компьютерной информации» посвящен анализу мер предупреждения мошенничества в сфере компьютерной информации. В процессе исследования автором выделена классификация мер предупреждения, а также высказано предположение, что повысить эффективность действующей на сегодняшний день в стране системы профилактики и предупреждения фактов мошенничества в сфере компьютерной информации можно путем разработки и внедрения в текущие процессы новых механизмов и методик деятельности государственных органов, в частности подразделений полиции и суда.

Параграф 2.3 «Личность осужденных за мошенничество в сфере компьютерной информации» посвящен изучению личности, лиц, осужденных по статье 159.6 УК РФ. На основании анализа данных судебной статистики и правоприменительной практики автором выделен типовой криминологический портрет личности осужденного по рассматриваемому виду преступления, который характеризуется главным образом средним

возрастом, высоким уровнем образования и положительной характеристикой индивидуальных качеств.

В работе приводятся примеры из правоприменительной практики, статистические данные и мнения исследователей в области уголовного права.

В заключении представлены краткие выводы по теме исследования.

Автор работы Гапонович К.В.

ОГЛАВЛЕНИЕ

ПЕРЕЧЕНЬ УСЛОВНЫХ ОБОЗНАЧЕНИЙ

УК – Уголовный кодекс Российской Федерации

УПК – Уголовно-процессуальный кодекс Российской Федерации

п. – пункт

ред. – редакция

РФ – Российская Федерация

ст. – статья

ч. – часть

ВВЕДЕНИЕ

Актуальность настоящего исследования состоит в том, что в условиях современной действительности большое значение придается именно компьютерным технологиям. Использование информационно-телекоммуникационных технологий в преступных целях в последние годы является серьезным вызовом как для правоохранительных, так и законодательных органов. Выступая на цифровом форуме в Сеуле, бывший Генеральный секретарь ООН Пан Ги Мун отметил, что революция в области информационно-коммуникационных технологий сопровождается новыми угрозами, связанными с киберпреступностью[1].

При этом одним из традиционных составов преступления как в России, так и во всем мире является мошенничество. В период компьютеризации неизбежным является развитие, эволюция видов и способов мошенничества, придавая ему дистанционный (цифровой, виртуальный) характер.

Так, анализ статистических данных МВД РФ свидетельствует об ухудшении динамики мошенничества в сфере компьютерной информации. В частности, за 2020 было зарегистрировано 761 преступление, связанное с мошенничеством в сфере компьютерной информации, что отражает рост уровня преступности на 10, 8 % по отношению к предыдущему отчетному периоду. За отчетный период с января по март 2021 года было зарегистрировано 166 преступлений, связанных с мошенничеством в сфере компьютерной информации, при этом прогнозируемый рост преступности по отношению к предыдущему отчетному периоду составил 16, 9 %.[2]

---

[1] Новости ООН [Электронный ресурс]: https://news.un.org/ru/story/2015/05/1263871#.VY5a1psdCt8 (дата обращения: 12.05.2021).

[2] Статистические сведения о состоянии преступности [Электронный ресурс] // Министерство внутренних дел РФ, URL: https://xn--b1aew.xn--p1ai/reports/item/23816756/ (дата обращения 12.05.2021 г.)

В данной связи мошенничество в сфере компьютерной информации требует активной разработки и выявления характерных особенностей преступлений, их состава, личности преступника и методов по предупреждению мошенничества.

Цель и задачи работы. Целью настоящего диссертационного исследования является комплексный анализ мошенничества в сфере компьютерной информации

Достижение поставленной цели предопределило необходимость решения следующих задач:

1) Отразить объективные и субъективные признаки мошенничества в сфере компьютерной информации;

2) Проанализировать субъективные признаки мошенничества в сфере компьютерной информации;

3) Провести отграничение мошенничества в сфере компьютерной информации от смежных составов преступлений;

4) Проанализировать состояние, структуру и динамику мошенничества в сфере компьютерной информации в России;

5) Исследовать меры предупреждения мошенничества в сфере компьютерной информации;

6) Отразить личность осужденных за мошенничество в сфере компьютерной информации.

Предметом исследования выступает совокупность уголовно-правовых норм, научные труды, статистические данные и судебная практика, отражающие специфику рассматриваемых правоотношений.

Теоретической базой исследования выступили труды отечественных правоведов, таких как В. К. Барчуков, И.Г. Гладких, М. Ю. Дворецкий, У. В. Зинина, Н. Д. Иващенко, Н. Н. Кадырова, В. Е. Козлов, С.Ю Кропачев, Н.Н. Кулешова, Т. М. Лопатина, В. И. Ляпунов, С. С. Медведев, Н. А. Подольный, М.Д. Фролов, Е.И. Христофорова и др.

Нормативной основой работы являются Уголовный кодекс Российской

Федерации, Уголовно-процессуальный кодекс Российской Федерации, а также ряд нормативно-правовых актов, регулирующих электронные средства платежа: Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31 июля 2020 г. N 259-ФЗ, Федеральный закон от 27 июня 2011 г. N 161-ФЗ (ред. от 22 декабря 2020 г.) «О национальной платежной системе».

Методологической основой исследования выступает общенаучный диалектический метод научного познания, предполагающий объективность и всесторонность познания исследуемых явлений. Вместе с тем автором применяются частно-научные методы: исторический, логический, системно-структурный, формально-юридический, сравнительно-правовой**.**

Эмпирическую основу исследования составили:

- материалы судебной практики Верховного Суда РФ и судов общей юрисдикции Российской Федерации, опубликованные в государственной автоматизированной системе Российской Федерации «Правосудие», предметом рассмотрения которых послужили вопросы мошенничества в сфере компьютерной информации в количестве 38 дел за 2019 – 2020 годы;

– основные статистические показатели деятельности судов общей юрисдикции за 2018 – 2020 годы, опубликованные на сайте Судебного департамента при Верховном Суде Российской Федерации;

– статистические сведения о состоянии преступности за 2019 – первый квартал 2021 годы, опубликованные на сайте Министерства внутренних дел Российской Федерации.

Теоретическое и практическое значение исследования заключается в том, что выводы, сделанные в процессе разработки диссертации, значимо дополняют теоретические знания о нем. А это является основой для разработки новых методов раскрытия и предупреждения мошенничества в сфере компьютерной информации .

Структура диссертации. Структура магистерской диссертации

обусловлена предметом, целями и задачами исследования. Диссертация включает введение, две главы, содержащие шесть параграфов, заключение, список использованной литературы.

1 Уголовно – правовая характеристика мошенничества в сфере компьютерной информации

1.1 Объективные признаки мошенничества в сфере компьютерной информации

Если производить уголовно-правовую характеристику преступного деяния, то основополагающим моментом здесь выступает рассмотрение всех признаков, которые в своей совокупности образуют состав преступления.

Из общей теории уголовного права России следует, что состав преступления – это совокупность предусмотренных уголовным законом объективных и субъективных признаков, характеризующих общественно опасное деяние как преступление. При этом любой состав преступления обладает признаками, которые принято группировать по элементам состава: объекту, объективной стороне, субъекту и субъективной стороне[3].

Верное определение объективных и субъективных признаков позволит правильным образом квалифицировать деяние преступника и соответственно верно назначить уголовное наказание. Более того, верное установление признаков способствует тому, что правоприменитель будет в состоянии отграничить одно преступное деяние от другого[4].

Как известно объективные признаки состава преступления состоят из объективной стороны и объекта преступления. В первую очередь необходимо изучить то, что выступает в качестве объекта преступления, предусмотренного ст. 159.6 УК РФ.

Если сказать об объекте более обобщенно, тогда можно обратиться к части 1 статьи 2 УК РФ, в которой сказано, что объект преступления – это права и свободы человека и гражданина, собственность, общественный порядок и общественная безопасность, окружающая среда, конституционный строй Российской Федерации, мир безопасность человечества. Традиционно,

---

[3] Чучаев, А.И Комментарий к Уголовному кодексу Российской Федерации (постатейный) /А.И. Чучаев М.: Норма, 2015. – С. 7.

[4] Грунтов И.О. К вопросу о понимании объекта преступления в уголовном праве /И.О. Грунтов // Труд. Работа. Профсоюз. Общество. – 2017. – № 2(56). – С. 41.

в соответствии со структурой УК РФ, выделяются общий, видовой, и непосредственный объекты преступления.

В названии разделов УК РФ обозначен родовой (специальный) объект, а глав УК РФ – видовой (групповой) объект преступлений.

Так, под «родовым объектом» понимается группа однородных общественных отношений, которые в силу однородности охраняются единым комплексом взаимосвязанных уголовно-правовых норм, содержащихся в определенном разделе УК РФ.

Статья 159.6 УК РФ находится в разд. VIII «Преступления против собственности», что позволяет обозначить родовой объект этой группы преступлений как совокупность общественных отношений, обеспечивающих защиту права собственности граждан.

Вместе с тем вопрос об объекте мошенничества в сфере компьютерной информации выступает дискуссионным. Так по мнению В. И. Гладких, чрезвычайно трудно сформулировать объект и предмет деяния, указанного в ст. 159.6 УК РФ. Автор поясняет, что общеизвестное представление о непосредственном объекте мошенничества как конкретной форме собственности вступает в противоречие с действующей редакцией компьютерного мошенничества, поскольку сфера компьютерной информации относится совершенно к другой области общественных отношений, а именно к тем отношениям, которые подвергаются воздействию со стороны преступлений, предусмотренных главой 28 УК РФ «Преступления в сфере компьютерной информации»[5].

Второй распространённой точкой зрения выступает, то что рассматриваемое преступление является двухобъектным. Основной объект - общественные отношения, связанные с отношениями собственности, независимо от ее формы, дополнительный — правоотношения, обеспечивающие информационную безопасность.

---

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

Так, по мнению А. Г. Безверхова, в условиях поступательного движения современной России к постиндустриальному обществу, постепенного перехода нашей страны к использованию высоких технологий повышается опасность «компьютерного мошенничества». Такое деяние характеризуется дополнительным объектом. Им выступает общественная безопасность[6].

Также О. М. Сафонов отмечает, что из самого названия ст. 159.6 УК РФ видно, что она предусматривает ответственность за деяния, нарушающие общественные отношения как в сфере собственности, так и в сфере безопасности компьютерных систем. На этом основании автор делает вывод, что данное преступление является двуобъектным, основным непосредственным объектом которого являются отношения собственности, а дополнительным - отношения в сфере безопасности компьютерных систем[7].

Между тем в научной среде существует и третий подход к определению объекта рассматриваемого преступления. Так Т. М. Лопатина считает, что основным непосредственным объектом компьютерного мошенничества являются отношения, охраняющие право собственности, а факультативным объектом - общественные отношения в сфере компьютерной информации[8]. Таким образом, по мнению Т.М. Лопатиной неправомерный доступ и модификация компьютерной информации не является обязательным признаком рассматриваемого состава преступления, что представляется не вполне верным.

Для более точного определения объекта рассматриваемого преступления обратимся к постановлению Пленума Верховного Суда

---

[6] Безверхов А. Г. Мошенничество и его виды: вопросы законодательной регламентации и квалификации // Уголовное право. 2015. №5. С.13.

[7] 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 - 116.

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

Российской Федерации в постановлении от 30 ноября 2017 года № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате». Пункт 20, который раскрывает вмешательство в средство хранения, обработки или передачи компьютерной информации действие, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации.

Аналогичной точки зрения придерживается и актуальная судебная практика, в абсолютном большинстве проанализированных автором судебных дел за 2020 г., опубликованных в системе ГАС «Правосудие», злоумышленники совершали преступление путем ввода или модификации информации платежных систем, баз данных и электронных ресурсов. К примеру «неправомерно вошел в модуль SBMS, который используется для внесения изменений в список услуг и проведения абонентских операций с номерами клиентов ПАО «<данные изъяты>», где, не имея соответствующего заявления клиента выбрал абонентский номер № с целью проведения модификации компьютерной информации модуля SBMS»[9].

В данной связи, автор диссертационного исследования придерживается позиции того, что рассматриваемое преступление является двухобъектным. Основной объект - общественные отношения, связанные с отношениями собственности, независимо от ее формы, дополнительный — правоотношения, обеспечивающие информационную безопасность.

Вторым дискуссионным вопросом в части объективных признаков состава мошенничества в сфере компьютерной информации представляется предмет, рассматриваемого преступления.

Ввиду того, что зачастую предметом рассматриваемого преступления выступают электронные денежные средства, то в науке уголовного и гражданского права существуют дискуссии могут ли безналичные средства платежа выступать объектами права и являться предметами преступлений.

---

[9] Приговор Центрального районного суда г. Тольятти Самарской области №1-262/2020 от 14 мая 2020 года [Электронный ресурс] // ГАС «Правосудие» URL: https://bsr.sudrf.ru/bigs/portal.htm (дата обращения 19.05.2021 г.)

Так М. А. Коростелев пишет, что безналичные и электронные деньги не могут являться объектом права собственности. Безналичные и электронные деньги не являются вещью, тогда как только вещь как телесный предмет может быть объектом права собственности[10].

Между тем статья 123 ГК РФ в объекты гражданских прав, а именно имущественные права: безналичные денежные средства, бездокументарные ценные бумаги и цифровые права[11]. В данной связи электронные денежные средства и бездокументарные ценные бумаги, безусловно выступают предметом рассматриваемого преступления, имущественную ценность электронных средств платежа подтверждается также в ст. 3 и ФЗ «О национальной платежной системе»[12].

Более актуальным в настоящее время представляется вопрос регулирования и рассмотрения в качестве предмета преступления криптовалюты. Объем капитализации криптовалют в настоящее время превысил 2 триллиона долларов, а компании PayPal и Tesla признали криптовалюты в качестве средств платежа[13]. Согласно позиции Министерства юстиции РФ «криптовалюта может быть квалифицирована как объект гражданских прав в качестве «иного имущества», так как она способна к обособлению и имеет имущественную ценность»[14]. Аналогичной позиции придерживается и судебная практика так постановлением

---

[10] Коростелев М. А. Правовой режим электронных денег в гражданском законодательстве: автореф. дис. . канд. юрид. наук. М., 2015. С. 11.

[11] Гражданский кодекс Российской Федерации (часть первая): федер. закон от 30 нояб. 1994 г. № 51-ФЗ: (ред. от 31 июля. 2020 г.) // КонсультантПлюс: справ. правовая система. − Версия Проф. − М., 2020. – Режим доступа: локальная сеть Науч. б-ки Том. гос. ун-та.

[12] Федеральный закон от 27 июня 2011 г. N 161-ФЗ (ред. от 22 декабря 2020 г.) «О национальной платежной системе» (с изм. и доп., вступ. в силу с 01 января 2021 г.) // КонсультантПлюс: справ. правовая система. − Версия Проф. − М., 2020. – Режим доступа: локальная сеть Науч. б-ки Том. гос. ун-та.

[13] Капитализация валют впервые превысила $ 2 трлн [Электронный ресурс] // Телеканал «РБК». - URL:https://www.rbc.ru/crypto/news/606b2d0a9a794773b0013395 (дата обращения 19.05.2021 г.)

[14] Егорова М. А., Кожевина О. В. Место криптовалюты в системе объектов гражданских прав // Актуальные проблемы российского права. — 2020. — Т. 15. — № 1. — С. 81—91, с 85

арбитражного апелляционного суда от 7 мая 2018 г. криптовалюта была включена в конкурсную массу должника и определена как иное имущество[15].

Между тем анализ Федерального закона от 31.07.2020 N 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[16] позволяет сделать вывод, о том что российское законодательство рассматривает криптовалюту как объект инвестирования, но не как средство платежа. При этом проводить сделки купли-продажи и обмена активов могут только российские банки и биржи, зарегистрированные в специальных реестрах Центрального банка РФ, что значительно сокращает виды криптовалют, как объектов права. Тем не менее представляется верным, что отдельные виды криптовалют, зарегистрированные надлежащим образом в Российской Федерации, должны выступать предметом рассматриваемого преступления ввиду их имущественной ценности, как объекта инвестирования.

Анализируя судебную практику по рассматриваемому виду преступления, следует прийти к выводу, что в подавляющем количестве случаев предметом рассматриваемого вида преступления выступают электронные денежные средства. К примеру, «с целью хищения электронных денежных средств, продолжая свой преступный корыстный умысел, осуществили ввод компьютерной информации в виде логинов и паролей»[17]. Тем не менее на практике также встречаются случаи неправомерного завладения ценными бумаги, в частности билетами на самолет, поезда дальнего следования, театры и т.д. Так, «путем незаконного вторжения в компьютерную информацию этих организаций и оформления от имени

---

[15] Постановление Девятого арбитражного апелляционного суда от 15 мая 2018 г. № 09ап-16416/2018 по делу № 40-124668/2017 [Электронный ресурс] // СПС «КонсультантПлюс».

[16] Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31 июля 2020 г. N 259-ФЗ // КонсультантПлюс: справ. правовая система. Версия Проф. М., 2020. Режим доступа: локальная сеть Науч. б-ки Том. гос. ун-та.

[17] Приговор Куйбышевского районного суда г. Омска № 1-9/2020 г. от 22 июня 2020 года [Электронный ресурс] // ГАС «Правосудие» URL: https://bsr.sudrf.ru/bigs/portal.htm (дата обращения 19.05.2021 г.)

организаций железнодорожных билетов с последующим возвратом и получением наличных денежных средств, эквивалентных стоимости билетов»[18].

Таким образом наиболее типичным предметом посягательства рассматриваемого вида преступления выступают электронные денежные средства и ценные бумаги, обладающие высокой ликвидностью.

Объективная сторона мошенничества в сфере компьютерной информации отличается собственной уникальностью. Так, без изменения остаются формы мошенничества (хищение и приобретение права на чужое имущество), исключаются общие способы совершения деяния (обман, злоупотребление доверием)[19]. Вместо них объективная сторона характеризуются следующими способами:

1) ввод, удаление, блокирование, модификация компьютерной информации либо

2) иное вмешательство.

Чтобы понимать в полном объеме особенности объективной стороны рассматриваемого деяния, необходимо раскрыть каждый из терминов, приведенных в диспозиции ст. 159.6 УК РФ.

Так, ввод следует расценивать, как внесение информации в определенную базу данных посредством использования дополнительных устройств (клавиатура, компьютерная мышь) с последующей записью внесенных сведений в этой базе. Блокирование подразумевает под собой создание обстоятельств, которые будут препятствовать доступу к информации для другого пользователя, расположенной на компьютере, несмотря на тот факт, что при блокировании такая информация сохраняется.

---

[18] Приговор Куйбышевского районного суда г. Новокузнецка № 1-9/2020 от 29 августа 2020 года [Электронный ресурс] // ГАС «Правосудие» URL: https://bsr.sudrf.ru/bigs/portal.htm (дата обращения 19.05.2021 г.)

[19] Иващенко Н.Д. Мошенничество в сфере компьютерной информации: проблемные вопросы // Столица науки. 2020. № 6. С. 269-276.

В свою очередь под модификацией необходимо понимать любое видоизменение информации, в том числе и ее объема при помощи использования компьютерных технологий. Термин «удаление» не вызывает особых затруднений, поскольку предполагает полное уничтожение информации с компьютерного устройства. Однако имеют место быть случаи, когда становится возможным восстановить ту информацию, которая была удалена.

Таким образом, как видно из изложенного, указанные действия оказывают непосредственное воздействие именно на информацию, расположенную на компьютере. Однако законодатель также обозначает, что возможно и иное вмешательство, не раскрывая при этом, что именно следует понимать под таким иным вмешательством. Поскольку в уголовном законе не содержится точного ответа на данный вопрос, в науке права приводятся различные точки зрения относительно видов иного вмешательства.

Так, большинство исследователей сходятся во мнении в том, что иное вмешательство следует расценивать, как любое воспрепятствование нормальному процессу функционирования информационной или информационно-телекоммуникационной сети.

Однако эта позиция не является единственной и, анализируя научные публикации можно также встретить мнение о том, что иное вмешательство предполагает также и любое незаконное воздействие на проводимые в отношении информации процессы, которые мешают ее нормальному использованию. Кроме этого, ученые также в большинстве своем сходятся во мнении, что такие иные вмешательства чаще всего совершаются именно при помощи ввода, хотя не исключены и иные способы[20].

Как известно, мошенничество предполагает наличие такого признака, как обман. Обман в свою очередь подразумевает сообщение или предоставление кому-либо тех сведений, который не отвечают

[20] Степанова К.В. Мошенничество в сфере компьютерной информации: российский и зарубежный опыт // Актуальные проблемы уголовного права, уголовного процесса и криминалистики. 2019. С. 32-38.

действительности. На основании предоставления таких сведений происходит введение в заблуждение потерпевшего лица. Стоит при этом подчеркнуть, что многие авторы говорят об отсутствии признака обмана применительно к мошенничеству в сфере компьютерной информации, поскольку как таковой потерпевший в этом посягательстве отсутствует именно относительно введения его в заблуждение. Специфика данного преступления несколько иная – не происходит обман или злоупотребление доверием потерпевшего – атаке подвергаются определенные информационные системы. О чем более подробно будет рассмотрено далее. Однако стоит здесь согласиться с мнением М.В. Степанова, который справедливо отмечает: «о каком обмане или злоупотреблении доверием можно вести речь, если отсутствует лицо, которому сообщаются ложные или несоответствующие действительности сведения»[21].

Необходимо также отметить, что способ совершения рассматриваемого преступления аналогичен объективной стороне. И способами как раз таки выступают ввод, удаление, блокирование, модификация информации и иные действия, которые в итоге образуют объективную сторону рассматриваемого посягательства[22].

С целью уточнения наиболее типичного способа совершения преступления, предусмотренного ст. 159.6 УК РФ, обратимся к материалам судебной практики. Анализ судебной практики позволяет сделать вывод, что в подавляющем количестве случаев преступление совершается путем ввода и модификации информации в корпоративные базы данных компаний. Как правило преступники, являются работниками данных компаний и используют свое служебное положение с целью неправомерного завладения денежными средствами клиентов. Так, «умышленно из корыстной

---

[21] Степанов М.В. Критический анализ нормы о мошенничестве в сфере компьютерной информации (ст. 159.6 УК РФ) // Юридическая наука и практика: Вестник Нижегородского академии МВД России. 2016. № 1. 174.

[22] Куликов А.В., Гуц Е.А. Мошенничество в сфере компьютерной информации // Известия тульского государственного университета. экономические и юридические науки. 2020. № 1. С. 82.

заинтересованности, используя свое служебное положение, с целью неправомерного доступа к охраняемой законом компьютерной информации, содержащей персональные данные клиентов ПАО «Вымпелком» и персональные данные их лицевых счетов, с целью ее модификации, под своими индивидуальными и учетными данными осуществила доступ в компьютерную программу «1С»,»[23]. Косвенное подтверждение данного вывода обосновывается материалами судебной практики, так за 2020 год по ч. 3 ст. 159 УК РФ, квалификация которой включает в себя, в том числе, использование служебного положения было осуждено 11 лиц из 29 человек общего количество осужденных.

Второй типичный способ совершения преступления стоит характеризировать по смыслу п. 20 Постановления Пленума Постановление Пленума Верховного Суда РФ от 30.11.2017 N 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», как вмешательство, а именно целенаправленное воздействие программных и программно-аппаратных средства на серверы, средства вычислительной техники и информационно-телекоммуникационные сети.

Злоумышленники, используя вредоносное программное обеспечение, взламывают считывающие устройства банкоматов, электронные базы данных и систему защиты аккаунтов. К примеру, «Осуществил ввод компьютерной информации, а именно привнесение новых последовательных электронных сигналов в систему хранения информации с помощью средств ввода, а именно: клавиатуры и соответствующей программы считывания графической информации»[24]. Также распространённым способом совершения анализируемого преступления выступает создание так называемых «фишинг-сайтов», то есть электронных ресурсов внешне схожих с официальным

[23] Приговор Октябрьского городского суда РБ 29 июля 2020 года. № 1-243/2020 [Электронный ресурс] // ГАС «Правосудие» URL: https://bsr.sudrf.ru/bigs/portal.htm (дата обращения 19.05.2021 г.)

[24] Приговор Видновского городского суда Московской области Дело № 1-183/2020 от 28 июля 2020 г. № 1-243/2020 [Электронный ресурс] // ГАС «Правосудие» URL: https://bsr.sudrf.ru/bigs/portal.htm (дата обращения 19.05.2021 г.)

электронными ресурсами платежных систем и популярных социальных сетей, которые содержат вредоносное программное обеспечение. К примеру, «посредством рассылки на используемые ими абонентские номера sms-сообщений определенного вида, содержащих ссылку для перехода на сайт «Интернет» - ресурса специального вредоносного компьютерного программного обеспечения.»[25].

Сходная судебная практика наблюдается также и на территории Томской области. Так, к примеру, Советский районный суд г. Томска рассмотрел уголовное дело в отношении подсудимых К.Р., Г.К. и Г.С. Как было установлено обстоятельствами дела указанные подсудимые на смартфоны потерпевших устанавливали вредоносное программное обеспечение. В силу установки такого обеспечения происходила автоматическая рассылка сообщений с целью снять с банковского счета потерпевших определенную денежную сумму. Подчеркнем при этом, что на стадии предварительного расследования такие действия были расценены, как кража по ст. 158 УК РФ. Такая квалификация произошла по той причине, что в материалах дела не имелось указание на применение обозначенных в ст. 159.6 УК РФ способов (ввод, модификация и т.д.). Однако впоследствии суд переквалифицировал содеянное именно на ст. 159.6 УК РФ, обозначив при этом, что отсутствие в обвинительном заключении слов «ввод», «модификация», «блокирование» компьютерной информации не говорит о том, что эти действия не были совершены и материалами дела этот факт подтвердился[26].

Также стоит отметить, что рассматриваемый вид мошенничества является весьма своеобразным, поскольку в классическом понимании мошенничество подразумевает, что именно с участием потерпевшего оно и

---

[25] Приговор Центральный районный суд города Кемерово № 1-573/2020 от «08» сентября 2020 года [Электронный ресурс] // ГАС «Правосудие» URL: https://bsr.sudrf.ru/bigs/portal.htm (дата обращения 19.05.2021 г.)

[26] Апелляционное определение Томского областного суда от 12.10.2017 по делу № 22-1652/2017 // КонсультантПлюс: справ. правовая система. Версия Проф. М., 2020. Режим доступа: локальная сеть Науч. б-ки Том. гос. ун-та.

произошло, поскольку имели место или обман потерпевшего, или же злоупотребление доверием. Однако мошенничество в сфере компьютерной информации возможно совершить и без участия потерпевшего, а лишь с использованием принадлежащей ему информации и при помощи компьютерных технологий. Конечно, в данном виде мошенничества есть и обман, но он здесь имеет место не в традиционном понимании – обман тут производится не потерпевшего, а определенной системы, к примеру, банковской. Именно на этом основании данный вид мошенничества специфичен по отношению к преступлению, обозначенному в ст. 159 УК РФ.

Что касается состава мошенничества в сфере компьютерной информации, то он материальный, поскольку для возможности привлечения лица к ответственности важно наступление именно общественно опасных последствий, то есть причинения потерпевшему ущерба. Оконченным такое преступление считается в тот момент, когда произошло, например, списание денежных средств со счета потерпевшего.

Таким образом, в завершение данного параграфа необходимо отметить, что мошенничество в сфере компьютерной информации посягает в первую очередь на отношения против собственности, о чем говорит включение нормы, предусматривающей ответственность за его совершение в главу 21 УК РФ. Однако присутствует и дополнительный — правоотношения, обеспечивающие информационную безопасность. Кроме этого, мошенничество в сфере компьютерной информации предполагает выполнение именно активных действий со стороны субъекта преступления. Предметом данного вида мошенничества является чужое имущество и право на чужое имущество, а также компьютерная информация, с помощью которой виновный осуществляет обманные действия и завладевает имуществом или приобретает право на имущество.

1.2 Субъективные признаки мошенничества в сфере компьютерной информации

Всяким преступлениям, нашедшим свое место в отечественном уголовном законодательстве, характерны не только объективные признаки, но и субъективные, а это значит, что исследуемый состав преступления также имеет свои субъекта и субъективную сторону.

Что касается непосредственно термина «субъект преступления», то его определение закреплено в Общей части УК РФ, а именно ст. 19 регламентирует признаки, характерные для лица, совершившего посягательство.

Субъект преступления – это элемент состава преступления, объединяющий признаки, характеризующие лицо, совершившее преступное посягательство. К признакам субъекта преступления относятся: его физическая природа, возраст, вменяемость и признаки специального субъекта. Имеются в виду следующие признаки: физическое лицо, признание гражданина вменяемым, достижение требуемого возраста. Эти характеристики обязательны для любого субъекта.

Что касается возраста субъекта, то общий возраст, установленный ч.1 ст.20 УК РФ – 16 лет. Перечисленные признаки субъекта относятся к общим и, следовательно, характерны для субъектов всех, предусмотренных Особенной частью УК РФ, составов преступлений.

Привлечь к ответственности за совершение рассматриваемого преступного посягательства возможно лицо, которое уже достигло возраста шестнадцати лет. При этом гражданство виновного (его наличие) значения не имеет. Таким образом, субъект в данном случае общий, поскольку возраст уголовной ответственности в исследуемом случае равен тому, который имеет место быть по общему правилу.

Следует отметить, что в доктрине уголовного права обосновывается предложение о необходимости понижения возраста уголовной ответственности за мошеннические действия. Так, С. С. Медведев пишет: «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»[27].

Между тем подобный подход представляется не обоснованным, поскольку как известно при дифференциации возраста ответственности учитывается возможность несовершеннолетних по-разному воспринимать и оценивать различные правовые запреты. Как уже было разобрано в предыдущем параграфе данного диссертационного исследования, объект анализируемого преступления представляет является двухобъектным и сложным для понимания. Несмотря на отмеченный С.С. Медведевым процесс информатизации общества, тем не менее существует ряд отдаленных населенных пунктов и семей, которые не пользуются персональными компьютерами и глобальным интернетом. Злоумышленникам и в настоящее время не составляет труда вводить в заблуждение доверчивых и не образованных в области информационной безопасности граждан, а вовлечь несовершеннолетних в совершение преступных действий, предусмотренных ст. 159.6 УК РФ им также не составит труда.

Более того следует отметить, что ч. 2 ст. 20 УК РФ не содержит общий состав мошенничества, в связи с чем снижение уголовной ответственности за деяние, предусмотренное ст. 156.9 УК РФ противоречит принципу справедливости по отношению к общему составу мошенничества.

Далее важным критерием субъективной стороны является вменяемость. В теории уголовного права вменяемость можно обозначить как медицинский

---

[27] Медведев С. С. Мошенничество в сфере высоких технологий: автореф. дис. . канд. юрид. наук. Краснодар, 2008. С. 15.

критерий, позволяющий установить, что привлекаемое к ответственности лицо является психически здоровым человеком, который в состоянии отдавать отчет совершаемым поступкам и имеет возможность ими руководить.

В уголовном законодательстве нет закрепленного понятия вменяемости и вменяемого лица, есть только понятие невменяемости. Российское уголовное законодательство содержит в себе императивные нормы о том, что невозможно привлечь к уголовной ответственности лицо в том случае, если оно не отвечает критериям вменяемости, либо же являлось невменяемым в тот момент, когда происходило преступления, в данном случае мошенничество, предусмотренное ст. 159.6 УК РФ. Невменяемость, как правило, возникает вследствие психического расстройства, слабоумия или иных факторов. Однако говорить о невменяемости лица допустимо исключительно на основании экспертного заключения. Кроме того, если говорить о привлечении лица к ответственности, то его вменяемость должна быть определена именно по отношению к совершенному посягательству. Иными словами – в момент совершения преступления лицо должно быть вменяемым и этот факт необходимо при наличии к тому оснований подтвердить экспертным заключением. То есть именно в момент совершения преступления лицо должно понимать характер своих действий, чтобы в последующем его можно было привлечь к уголовной ответственности.

Согласно п. 3 ст. 196 Уголовно-процессуального кодекса от 18.12.2001 N 174-ФЗ[28] (далее – УПК РФ) назначение и производство судебной экспертизы обязательно, если необходимо установить психическое состояние обвиняемого, когда возникает сомнение в его вменяемости или способности самостоятельно защищать свои права и законные интересы в уголовном судопроизводстве. Неустановление психического состояния лица,

[28] Уголовно-процессуальный кодекс Российской Федерации: федер. закон от 18 декабря 2001г. N 174-ФЗ: (ред. от 05 апреля 2021г., с изм. От 13 апреля 2021 г.) // КонсультантПлюс: справ. правовая система. Версия Проф. М., 2020. Режим доступа: локальная сеть Науч. б-ки Том. гос. ун-та.

привлекаемого к уголовной ответственности, препятствует постановлению законного и обоснованного судебного решения. В данной связи необходимость проведение судебно-психиатрической экспертизы, в ряде случаев, необходимо также и в достаточно сложным в интеллектуальном плане мошенничестве в сфере компьютерной информации. К примеру, «согласно заключению судебно-психиатрической комиссии экспертов № 2495 от 03.10.2018, Соловьев С.Н. мог в полной мере осознавать фактический характер и общественную опасность своих действий и руководить ими, как в момент инкриминируемого ему деяния, так и в настоящее время, в принудительных мерах медицинского характера не нуждается»[29].

Как уже отмечалось, субъектом преступления, предусмотренного ст. 159.6 УК РФ, является физическое вменяемое лицо, достигшее 16-летнего возраста.

Важно при этом отметить, что помимо календарного возраста, уголовный закон называет психологический возраст, что следует из ч. 3 ст. 20 УК РФ. Если несовершеннолетний достиг возраста уголовной ответственности, но вследствие отставания в психическом развитии, не связанном с психическим расстройством, что установлено судебной комплексной психолого-психиатрической экспертизой, не мог в полной мере осознавать фактический характер и общественную опасность своих действий (бездействия) либо руководить ими, то он не будет подлежать уголовной ответственности. То есть психически ребенок здоров, но жизненного опыта, присущего сверстникам, не получил, оценивать последствия своих поступков пока еще не способен, а значит, является «невменяемым по возрасту».

Кроме этого, стоит акцентировать внимание на том, что, если речь идет о совершении действий, предусмотренных ч. 3 ст. 159.6 УК РФ, то в данном случае может фигурировать и специальный субъект – лицо, занимающее

---

[29] Приговор Ленинского районного суда г. Тюмени № 1-886/2019 от 9 июля 2019 года [Электронный ресурс] // ГАС «Правосудие» URL: https://bsr.sudrf.ru/bigs/portal.htm (дата обращения 19.05.2021 г.)

служебное положение. Между тем, как уже отмечалось в предыдущем параграфе настоящей работы, лицо занимающее служебное положение один из основных субъектов анализируемого преступления. При это по смыслу п. 29 Пленума ВС РФ, не обязателен доступ должностного лица к непосредственному управлению денежных средств. Получение финансовой выгоды может быть вторичным по отношению к внесенным изменения в электронную отчётную документацию и единые базы данных, между тем вносимые изменения должны преследовать корыстную цель. К примеру, показателен следующий случай, «путем ввода и модификации компьютерной информации, с использованием своего служебного положения, а именно путем внесения в ПИРО «Алушта» не соответствующих действительности данных о якобы выполнении некоторыми военнослужащими войсковой части 71316 высшего квалификационного уровня физической подготовленности, что послужило основанием для выплаты этим военнослужащим»[30].

Далее следует рассмотреть субъективную сторону преступления. Этот признак отражает то состояние, которое имеет место быть у обвиняемого, его психическое внутреннее чувство к совершаемому.

Субъективная сторона любого преступления подразумевает под собой именно то психическое и внутреннее состояние субъекта преступления, которое имело место быть в момент совершения посягательства. В рамках субъективной стороны происходит установление отношения преступника к тому, что он совершил.

Крайне важно отметить здесь тот факт, что не любое психическое состояние лица при оценке содеянного будет рассматриваться, как субъективная сторона. Рассмотрение особенностей психики субъекта затрагивает лишь тот временной промежуток, в рамках которого совершалось преступное деяние. Как правило, субъективная сторона состоит

---

[30] Приговор Магнитогорского гарнизонного военного суда № 1-15/2019 от 14 марта 2019 г. [Электронный ресурс] // ГАС «Правосудие» URL: https://bsr.sudrf.ru/bigs/portal.htm (дата обращения 19.05.2021 г.)

из нескольких элементов, куда входят вина, мотив и цель, которыми руководствовался преступник. Однако мотив и цель являются факультативными признаками и их установление требуется не всегда. Определению мотива и цели стоит уделять особое внимание в том случае, когда в норме Особенной части УК РФ эти аспекты выступают в роли квалифицирующих признаков. Относительно рассматриваемого посягательства следует отметить, что мотив и цель при оценке содеянного не имеют значения, поскольку более серьезное наказание за их наличие в ст. 159.6 УК РФ не предусмотрено[31].

Субъективная сторона непосредственно мошенничества в сфере компьютерной информации характеризуется умышленной виной.

Вид же умысла в доктрине уголовного права является дискуссионным. 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[32].

Между тем 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[33]. Таким образом преступник понимает и в полной мере осознает, что выполняемые им действия носят характер преступных и за это последует применение мер уголовной

---

[31] Уголовное право России. Общая часть: учебник для академического бакалавра/ под ред. О.С. Капинус. – М. Издательство Юрайт, 2015. Серия: Бакалавр. Академический курс. – С.156.

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

[33] Фролов М. Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации: дис. ... канд. юрид. наук Москва, 2019. С 92.

ответственности[34]. Что касается волевого критерия, то в его рамках можно говорит, что, реализуя преступный умысел, преступник желает того, чтобы общественно-опасные последствия в результате наступили.

В продолжение вопроса корыстной цели в юридической науке существует дискуссионный вопрос: является ли корыстным изъятие чужого имущества без цели обратить его в свою пользу, к примеру, передать в пользование другим лицам, уничтожить кредитные обязательства и т.д.?

Автору в данном случае близка позиция Л. В. Иногамовой-Хегай, что для квалификации мошенничества корысть есть, когда виновный отдает чужое имущество не только близким, но и другим лицам, к судьбе которых у него есть какой-то интерес: симпатии, сострадание, бравирование и др[35].

Обязательность корыстной цели при совершении мошенничества в сфере компьютерной информации отражено также и 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.

В завершение настоящего параграфа отметим, что мошенничество в сфере компьютерной информации может быть совершено как общим, так и специальным субъектом – при этом данный факт влияет на квалификацию преступления и совершение его специальным субъектом влечет более

---

[34] Кропачев С.Ю. Мошенничество в сфере компьютерной информации как угроза экономической деятельности: актуальные вопросы квалификации // Современная наука: актуальные проблемы теории и практики. серия: экономика и право. 2020. № 4. С. 184.

[35] Иногамова-Хегай Л. В. Мошенничество, присвоение, растрата: проблемы квалификации конкурирующих и смежных норм // Уголовное право. 2015. №5. С. 32.

строгое наказание. Кроме этого, субъективная сторона такого преступления – это прямой умысел с корыстной целью.

1.3 Отграничение мошенничества в сфере компьютерной информации от смежных составов преступлений

Введение в УК РФ ст. 159.6 произошло относительно недавно – в 2012 г. До 2012 года же подобного рода преступления квалифицировались в рамках главы 28 УК РФ «Преступления в сфере компьютерной информации». Несмотря на тот факт, что уже на протяжении более восьми лет мошенничество в сфере компьютерной информации выделено не только в отдельный состав, но и в другую главу, на практике до сих пор случаются проблемы относительно его отграничения от другого состава. На настоящий момент основное отграничение ст. 159.6 УК РФ следует проводить со ст. 272 УК РФ, поскольку именно эти два состава имеют схожие между собой черты. Однако при детальном рассмотрении это абсолютно два разных состава, разграничивать которые крайне необходимо, поскольку ответственность наступает за совершенно разные деяния.

Рассматриваемый в ч. 1 ст. 159.6 УК РФ основной состав предполагает две составляющие:

1) неправомерное завладение злоумышленником компьютерной информацией — в зависимости от характера преступления ответственность за данные действия наступает согласно ст. 272 либо ст. 273 УК РФ;

2) присвоение чужого имущества путем использования информации, полученной незаконным путем с целью хищения, например, денежных средств с банковской карты, — ответственность должна наступать согласно требованиям ст. 69 УК РФ по совокупности преступлений, в число которых войдет и ст. 159.6 УК РФ.

На приведенном примере можно выявить первые отличия указанных составов: касаемо объекта и предмета посягательства. Дело в том, что в ст. 272 УК РФ предметом посягательства является и информация, содержащаяся в компьютере, и компьютер, который выступает носителем информации, а объектом деяния выступают общественные отношения, обеспечивающие безопасность информации. В случае наличия состава ст. 159.6 УК РФ предметом деяния является полученная незаконным путем информации: ее используют для хищения или приобретения права на чужое имущество; тем самым общественные отношения, обеспечивающие сохранность чужого имущества, рассматриваются в качестве объекта.

Но при этом следует отметить, что безопасность компьютерной информации может выступать дополнительным объектом мошенничества, а хищение собственности — дополнительным объектом неправомерного доступа к компьютерной информации, совершенного с корыстными целями[36].

Так, Куницына Г.С. совершила неправомерный доступ к охраняемой законом компьютерной информации, что повлекло блокирование и уничтожение компьютерной информации при следующих обстоятельствах.

Куницина Г.С., обладая знаниями в области компьютерной техники, в корыстных целях использовала доступ к сети Интернет и сим-карту, а также сотовый телефон. В результате совершения противоправных действий в виде подбора пароля к электронному ящику Куницина получила доступ к компьютерной информации, которая подлежит защите на основании законодательства. После этого она изменила пароль от этого ящика, что привело к воспрепятствованию пользования им его владельцем Потерпевшей №1. Кроме этого, Куницина также удалила всю информацию, находящуюся в данном почтовом ящике, что привело в непригодное для использования состояние указанной информации, тем самым Куницына Г.С. осуществила

[36] Кулешова Н. Н., Христофорова Е. И. Особенности квалификации мошенничества в сфере компьютерной информации // Вопросы науки и образования. 2018. № 14 (26). С. 41-46.

неправомерный доступ к информации, блокирование и уничтожение информации, содержащейся в электронном почтовом ящике[37].

Обращаясь к разграничению ст. 159.6 и ч. 2 ст. 272 УК РФ, предусматривающей неправомерный доступ к компьютерной информации, совершенный с корыстными целями, можно сказать, что на первый взгляд объективная сторона рассматриваемых составов имеет много сходства. Но стоит учесть, что ввод, удаление, блокирование, модификация или любое иное вмешательство в информацию это лишь способ совершения мошенничества, в то время как, согласно диспозиции ст. 272 УК РФ, названные характеристики являются обязательными последствиями преступления, за которое наступает уголовная ответственность[38].

Здесь также стоит отметить, что одним из последствий деяния, предусмотренного ст. 272 УК РФ, выступает именно уничтожение информации. Диспозиция же ст. 159.6 УК РФ говорит о том, что мошенничество может быть совершено путем удаления информации. То есть уже на этом этапе видно различие между составами. Однако, правоприменитель зачастую не разграничивает между собой уничтожение информации и ее удаление, хотя по своей сущности — это абсолютно различные деяния. Уничтожение и удаление рассматриваются судами в каждом из этих случаев, как создание условий, при которых использование информации невозможно.

Так, Первоуральский городской суд Свердловской области рассматривал уголовное дело, в рамках которого происходило обвинение Поспелова И.Д. в том, что им было совершено несколько эпизодов преступных деяний, предусмотренных ч. 2 ст. 272 и ч.1 ст. 159.6 УК РФ. Как указывает суд в своем приговоре, в процессе рассмотрения дела установлен

---

[37] Приговор Дзержинского районного суда г. Оренбурга Оренбургской области от 28.01.2019 по делу № 1-504/2018. [Электронный ресурс] // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/smPVc9O2vldJ/ (дата обращения: 12.05.2021).

[38] Барчуков В. К. К вопросу о содержании признаков объективной стороны мошенничества в сфере компьютерной информации // Безопасность бизнеса. 2016. № 5.С. 41–46.

факт удаления, уничтожения информации, хранящейся на компьютере, что обусловило создание обстановки, при которой использование информации ее обладателем стало невозможно[39].

Однако уравнивание удаления и уничтожения информации видится необоснованным, особенно учитывая тот факт, что для одной статьи УК РФ удаление – это способ совершения деяния, а для другой уничтожение – это последствие преступного посягательства.

Разграничение стоит проводить и по субъективной стороне: деяние, предусмотренное ст. 159.6 УК РФ, характеризуется прямым умыслом, при этом обязательное условие состоит в том, что виновный руководствуется материальными целями. В отличие от мошенничества в сфере компьютерной информации при неправомерном доступе, согласно ч. 2 ст. 272 УК РФ, для преступника важно получение определенной информации, которая в дальнейшем поможет злоумышленнику получить выгоду имущественного характера, не связанную с незаконным приобретением имущества[40].

Различие существует и в санкциях. За основной состав мошенничества в сфере компьютерной информации самое строгое наказание не связано с лишением свободы, тогда как за неправомерный доступ размер наказания по ч. 2 ст. 272 УК РФ значительно строже: до четырех лет лишения свободы.

В разъяснениях постановления Пленума Верховного Суда РФ от 30 ноября 2017 г. «О судебной практике по делам о мошенничестве, присвоении и растрате»[41] обращается внимание на то, что мошенничество в сфере компьютерной информации, совершенное путем неправомерного доступа к

---

[39] Приговор Первоуральского городского суда Свердловской области от 30.04.2015 года по делу № 1-111/2015 // КонсультантПлюс: справ. правовая система. Версия Проф. М., 2020. Режим доступа: локальная сеть Науч. б-ки Том. гос. ун-та.

[40] Кадырова Н. Н., Захаров И. С. Некоторые аспекты «компьютерных преступлений» // Вестник Челябинского государственного университета. Серия «Право». 2018. Т. 3, № 3. С. 74–76.

[41] Постановление Пленума Верховного Суда РФ от 30.11.2017 N 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // КонсультантПлюс: справ. правовая система. Версия Проф. М., 2020. Режим доступа: локальная сеть Науч. б-ки Том. гос. ун-та.

ней или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по ст. 272, 273 или 274.1 УК РФ.

Здесь также стоит обратить внимание на то, что если лицо воспользовалось полученной информацией не с корыстными целями, то уголовная ответственность по ст. 159.6 УК РФ не наступает. До введения указанной статьи такое преступление квалифицировалось бы по совокупности с учетом требований ст. 272 (273) и 159 (158) УК РФ.

2 Криминологическая характеристика мошенничества в сфере компьютерной информации

2.1 Состояние, структура и динамика мошенничества в сфере компьютерной информации

Под состоянием преступности принято понимать количественные показатели, выражающиеся в абсолютных цифрах, которые отражают общее количество преступлений или их отдельных групп или видов и лиц, совершивших эти преступления, зарегистрированных за определенный период времени на конкретной территории[42].

Чтобы определить текущее состояние такого вида преступности, как мошенничество в сфере компьютерной информации, необходимо рассмотреть основные криминологические характеристики преступного

[42] Фомин С. А. Криминологические характеристики преступности и основные показатели характеристик преступности, ее отдельных групп и видов на современном этапе // Вестник Сибирского юридического института МВД России. 2018. №1 (30) с. 95

явления и выделить его характерные признаки. В юридической науке криминологическая характеристика преступлений в сфере компьютерной информации представляет собой совокупность признаков, характерных этому виду правонарушений, которые могут использоваться в качестве оснований для разработки теорий о личности преступника и событиях совершения преступления, с помощью которых можно оценить необходимость применения тех или иных мер в процессе расследования преступлений[43].

С целью расчета современного состояния мошенничества в сфере компьютерной информации обратимся к статистическим данным Министерства внутренних дел Российской Федерации. Так за январь-март 2021 г. в России было зарегистрировано 166 преступлений, что составляет около 0, 11 зарегистрированных преступлений на 100 тыс. жителей. За январь-декабрь 2020 г. в России было зарегистрировано 761 преступление, связанных с мошенничеством в сфере компьютерной информации, что составляет порядка 0,52 зарегистрированных преступлений на 100 тыс. жителей[44].

Вместе с тем несмотря на сравнительно небольшой удельный вес зарегистрированных мошенничеств в сферы компьютерной информации следует не забывать о высокой латентности рассматриваемого вида преступления. Как показывают уголовная и судебная статистика, значительная часть таких преступлений остается за рамками реально выявленных и раскрытых[45].

В связи с этим растет уровень латентности преступлений в сфере компьютерной информации, что в свою очередь, становится причиной

---

[43] Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. М.: Горячая линия–Телком, 2002. – С. 114.

[44] Статистические сведения о состоянии преступности [Электронный ресурс] // Министерство внутренних дел РФ. URL: https://xn--b1aew.xn--p1ai/reports/item/23816756/ (дата обращения 12.05.2021 г.)

[45] Зинина У. В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном Аправе: автореф. дис. на соиск. учен. степ. канд. юрид. наук, М., 2007. 4 с.

отсутствия у государства достаточных данных для разработки и формирования эффективных в современных реалиях мер противодействия преступности в этой сфере и предупреждения новых преступлений.

Структура преступности представляет собой соотношение или удельный вес отдельных видов преступлений, выделенных по уголовно-правовым, криминологическим или смешанным критериям. Структура преступности выражается в абсолютных и относительных (в процентах) показателях, фактах совершенных преступлений и лицах, их совершивших[46].

Для отражения структуры мошенничества в сфере компьютерной информации проанализируем 2020 год. Так в 2020 году было зарегистрировано 761 рассматриваемых видов мошенничества, их удельный вес в общем количестве зарегистрированных преступлений составил 0,04 %. По отношению к общему виду мошенничеств, удельный вес мошенничества в сфере компьютерной информации составил 0, 23 %. По отношению к смежным составам преступлений, совершенных с использованием информационно - телекоммуникационных технологий или в сфере компьютерной информации, удельный вес мошенничества в сфере компьютерной информации составил 16, 92 %.

Среди лиц, совершивших мошенничество в сфере компьютерной информации, наибольший удельный вес в 2020 году составили мужчины - 93, 1 % от удельного количества рассматриваемого преступления., удельный вес женщин составил 6, 9 %.

По возрасту на момент совершения преступления Подавляющим количеством осужденных за преступление, предусмотренное ст. 159.6 УК РФ составляют преступники в возрасте от 18 до 24 в 2020 году их количество составило 12 человек, что составляет 41, 38% от общего числа осужденных, второй возрастной группой занимающей основной процент осужденных по

[46] Прозументов Л. М., Шеслер А.В. Криминология. Общая часть: Учебник. – Томск: ООО «ДиВо», 2007. С 64.

анализируемому составу преступления, выступили лица в возрасте 25-29 лет, их удельный вес от общего количества осужденных лиц составил 31, 03%.

Абсолютное количество осужденных 29 были постоянным жителями местности совершение преступления (100 %), также абсолютно число осуждённых лиц по данному составу преступления являлись гражданами РФ (100 %). Преобладающим уровнем образования лиц, совершивших рассматриваемое преступления, являлось средне - профессиональное образование им обладали 14 осужденных – 48, 28 % от общего числа осужденных. Характеризуя род занятий, осужденных следует отметить, что 13 лиц, то есть 44, 83 % от общего числа осуждённых лиц являлись трудоспособными лицами без постоянного источника дохода[47].

Проанализируем динамику рассматриваемого нами вида мошенничества за последние три года. Так согласно статистическим данным МВД РФ в 2019 году было зарегистрировано 687 преступлений, связанных с мошенничеством в сфере компьютерной информации, что было на 29, 2 % ниже, чем в предыдущем отчетном периоде. За 2020 было зарегистрировано 761 преступление, связанное с мошенничеством в сфере компьютерной информации, что отражает рост уровня преступности на 10, 8 % по отношению к предыдущему отчетному периоду. За отчетный период с января по март 2021 года было зарегистрировано 166 преступлений, связанных с мошенничеством в сфере компьютерной информации, при этом прогнозируемый рост преступности по отношению к предыдущему отчетному периоду составил 16, 9 %.

В целом анализ статистических данных динамики мошенничества в сфере компьютерной информации отражает стабильный рост темпов прироста регистрируемых преступлений.

В связи с чем наблюдается негативная динамика в развитии преступлений, рост преступности, постоянно совершенствуя и

---

[47] Сводные статистические сведения о состоянии судимости в России [Электронный ресурс] // Судебный департамент при Верховном Суде РФ. URL: https://xn--b1aew.xn--p1ai/reports/item/23816756/ (дата обращения 12.05.2021 г.)

видоизменяясь, опережает в темпы прироста населения. Новые виды и формы преступных деяний характеризуются изощренностью выбираемых правонарушителями методов, что в свою очередь становится причиной повышения степени общественной опасности преступлений и ущерба, который причиняется обществу в целом и его отдельным субъектам в частности. Пытаясь выиграть борьбу за право существования, преступники разрабатывают новые методики совершения посягательств, повышают уровень интеллектуальности преступности и активно используют в механизмах современные технологические разработки. Следует отметить, что реформирование преступной системы является не только причиной увеличения ее масштабов, но и влечет непрерывный процесс криминализации не известных ранее форм общественно опасных деяний[48].

На основании вышеизложенного отразим основные выводы рассматриваемой главы курсовой работы:

- Состояния преступления, связанных с мошенничества в сфере компьютерной информации, характеризуется сравнительно небольшим удельным весом, по отношению к остальным зарегистрированных преступлений, а также в количестве зарегистрированных преступлений на 100 тыс. жителей. Тем не менее мошенничество в сфере компьютерной информации характеризуется высокой латентностью и сложностью расследования отчего сравнительно невысокое количество регистрируемых преступлений не свидетельствует о низкой опасности рассматриваемого вида преступления.
- Структура мошенничества в сфере компьютерной информации характеризуется также сравнительно низким удельным весом по отношению к общему числу зарегистрированных преступлений, общему составу мошенничеству и смежным видам преступлений в сфере компьютерной информации. Данные о лицах, совершивших преступление характеризуются

[48] Курс мировой и российской криминологии в 2 т. Т. II. Особенная часть: учебник для вузов / В. В. Лунеев. — М.: Издательство Юрайт, 2015. С. 334.

преобладанием мужчин, как субъектов преступления. Возраст преступников в преобладающем количестве составлял от 18-24 лет, преобладающим уровнем образование выступило средне профессиональное. Преступления в абсолютном количестве случае совершалось в постоянном месте проживания преступника, также в подавляющем количестве осужденные являлись трудоспособными лицами без постоянного источника дохода.

- Динамика мошенничества в сфере компьютерной информации характеризуется сравнительно стабильным приростом регистрируемых преступлений, средний показатель темпа прироста за анализируемый период составил порядка 10%.

2.2 Предупреждение мошенничества в сфере компьютерной информации

Предупреждение мошенничества в сфере компьютерной информации реализуется через использование юридических, организационных и программно-технических норм. Юридическая сфера регулирования затрагивает вопрос ответственности за нарушения установленных законом рамок использования информационных технологий в различных сферах жизни общества[49].

Важным элементом обеспечения защиты в сфере компьютерной информации является охрана с помощью организационно-технических норм информационных центров, где кооперируется все совокупность получаемых компьютерных сведений.

---

[49] Гладких В.И. Компьютерное мошенничество: а были ли основания для криминализации? // Рос. следователь. – 2014. – № 22. – С. 25-31.

Со стороны разработчиков компьютерного обеспечения и различных информационных систем ведется работа по защите компьютерной информации от случайной утраты и умышленного на нее посягательства. Защита реализуется за счет разработки программного обеспечения, распознающего вредоносные механизмы, систем резервного копирования, сигнализирующих механизмов и т.д. На государственном уровне защита компьютерной информации осуществляется специально уполномоченными в этой сфере правоохранительными органами, в чьи обязанности входит разработка предупреждающих совершение преступлений процедур и расследование совершенных информационных правонарушений.

Под предупреждением преступности понимается совокупность всех законных видов, форм, способов, средств и методов контроля над преступностью независимо от того какой отраслью права они предусмотрены.[50]

Проблемой современного этапа предупреждения мошенничества в сфере компьютерной информации также является недостаточный уровень финансирования. Отсутствие соответствующей финансовой поддержки мер по предупреждению преступности является логичной причиной отсутствия в вооружении полномочных в борьбе с интернет-преступлениями государственных органов механизмов и методик расследования нарушений.

Преступность в компьютерной сфере распространяется с пугающей скоростью, затрагивая все больше сфер общественной жизни и причиняя им все больший вред. С развитием преступных схем мошенники не останавливаются на достигнутом и разрабатывают новые мошеннические механизмы завладения чужим имуществом и разрабатывают новые технические устройства и системы обмана граждан. В то же время информационно-техническое обеспечение правоохранительных органов не соответствует современным требованиям и не позволяет своевременно

[50] Н.В. Щедрин. Основы общей теории предупреждения преступности: Учеб. пособие / Краснояр. гос. ун-т, 1999. С. 7

реагировать на факты компьютерного мошенничества и препятствовать их совершению.

Мешает эффективному раскрытию изучаемого вида преступлений еще и разрозненность деятельности правоохранительных органов. Отечественное законодательство не закрепляет единой схемы действий в борьбе с преступлениями, не выявлена последовательность действий органов власти в случае получения информации о совершении преступления. В связи с тем, что правоохранительные органы по-разному реагируют на обнаруженные преступления, до сих пор не выработана единая эффективная практика по расследованию преступлений и их предупреждению[51]. Также отсутствует закрепление характерных признаков мошенничества в сфере компьютерной информации, способное определить пределы и правила квалификации преступлений.

С позиции Т.М. Лопатиной, система мер предупреждения компьютерных преступлений должна быть комплексной и включать в себя, с одной стороны, организационно-управленческие, технические (физические) меры, с другой — кадровые (в сочетании с морально-этическими) и правовые[52].

Классифицируем на данном основании следующие меры предупреждения мошенничества в сфере компьютерной информации

- меры общей превенции (например, политические, экономические, социальные, научно-технические, духовно-культурные)

- специальные превентивные меры (правовые, духовно-культурные, организационно-управленческие, технические, криминалистические и др.)[53].

---

[51] Гарбатович Д.А. Проблемные аспекты эффективности норм, предусматривающих ответственность за совершение преступлений в сфере компьютерной информации // Библиотека криминалиста. – 2013. – № 5. – С. 6-14.

[52] Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: дис. ... д-ра юрид. наук / Т.М. Лопатина. — М.: РГБ, 2007. — 418, с 316

Общепревентивные меры предупреждения компьютерных преступлений носят всеобщий характер и направлены на профилактику как компьютерной преступности в частности, так и преступности в целом. Разберем их подробней

- Общеполитическим мерам предупреждения преступлений в сфере компьютерной информации в России можно отнести: развитие демократии и гражданского общества, обеспечение незыблемости конституционного строя, территориальной целостности и суверенитета Российской Федерации.

- Общеэкономические превентивные меры включают: повышение конкурентоспособности национальной экономики; экономический рост, который достигается прежде всего путем развития национальной инновационной системы и увеличения инвестиций в человеческий капитал; повышение производительности труда.

- Общие социальные меры предполагают: снижение уровня социального и имущественного неравенства населения, стабилизацию его численности в среднесрочной перспективе, а в долгосрочной перспективе — коренное улучшение демографической ситуации; обеспечение личной безопасности, а также доступности комфортного жилья, высококачественных и безопасных товаров и услуг, достойной оплаты активной трудовой деятельности.

- Среди научно –технических меры общей превенции. Представляется наиболее перспективными внедрение механизмов по отслеживанию проходящей в компьютерной сети информации. С помощью этого элемента защитной системы государства представляется возможным использование алгоритмов вычисления совершающихся и планирующихся правонарушений, а также реализация контроля за деятельностью личностей, представляющих риск для информационно-технологической системы общества

- Духовно-культурные меры общей превенции включают: признание первостепенной роли культуры для возрождения и сохранения культурно-нравственных ценностей, укрепления духовного единства

многонационального народа Российской Федерации и международного имиджа России в качестве страны с богатейшей традиционной и динамично развивающейся современной культурой, создание системы духовного и патриотического воспитания граждан России.

Между тем наиболее специальные меры предупреждения преступности в сфере компьютерной информации.

- Правовые меры предупреждения преступности в сфере компьютерной информации характеризуются совершенствованием действующего законодательства с целью предупреждение и усиление эффективности действующего законодательства. Так, согласно нормам действующего на территории РФ Уголовного закона под преступлением в сфере компьютерной информации понимается реализованное преступным путем получение доступа к компьютерам и компьютерным сетям, которые характеризуются причинением жертве вреда в форме блокировки или неправомерного копирования размещенной на носителе информации[54]. Уголовную ответственность законодатель предусмотрел лишь за посягательства, которые квалифицируются как распространение вредоносных для информационных систем программ, незаконное завладение доступом к информации, нарушения, допущенные в процессе реализации деятельности на электронно-вычислительных машинах[55].

Этим УК РФ[56] ограничивается, что свидетельствует об отсутствии разработанных мер профилактики и предупреждения мошенничества в сфере компьютерной информации. Необходимо обеспечить бесперебойную деятельность правоприменительных представителей государственной власти

---

[54] Ляпунов Ю.И., Пушкин А.В. Преступления в сфере компьютерной информации. Уголовное право. Особенная часть [Текст] / Под ред. Н.И. Ветрова, Ю.И. Ляпунова. – М., 2016. – с. 540.

[55] Подольный Н.А. Отдельные проблемы расследования преступлений, совершённых с применением компьютерных технологий // Библиотека криминалиста. – 2013. -№ 5. – С. 116.

[56] Уголовный кодекс Российской Федерации: федер. закон от 13 июня 1996 г. N 63-ФЗ: (ред. от 05 апреля 2021г., с изм. от 08 апреля 2021 г.) //. КонсультантПлюс: справ. правовая система. Версия Проф. М., 2020. Режим доступа: локальная сеть Науч. б-ки Том. гос. ун-та.

в направлении разработки стандартов взаимодействия государственных структур и их совершенствования. Также представляется логичным выход на международный уровень, который возможен через внедрение идей стандартизации в проектирование деятельности Интерпола.

- Организационно-управленческие меры специального предупреждение, рассматриваемых преступлений имеют ведущее значение в системе мер предупреждения.

Так, некоторые отечественные специалисты, рассматривая вопрос предупреждения информационного мошенничества, предлагают создать систему государственных органов, в правомочия которых будет включена возможность запроса и получения от кредитных организаций информации, которая имеет статус банковской тайны, в определенные сроки и в конкретной форме. По мнению правоведов, такая разработка позволит сократить проблемы, возникающие в процессе взаимодействия правоохранительных органов и банковских структур. Передавать подобные сведения предлагается в целях сокращения сроков рассмотрения дел и рационализации процесса на электронных носителях.

Еще одним важным направлением предупреждения преступности является обеспечение эффективного взаимодействия правоприменительных органов государственной власти – судов и подразделений системы правоохранительных органов. Добиться этого возможно с помощью внедрения в практику единых регламентов, определяющих требования, правила и рамки такого взаимодействия. Также необходимо организовать работу названных структур в соответствии с потребностями современного общества, обеспечив правоприменителей необходимой базой информационного и технического оснащения[57].

На основании вышеизложенного классифицируем меры предупреждение мошенничества в сфере компьютерной информации на:

---

[57] Дворецкий М.Ю., Стромов В.Ю. Эффективная реализация уголовной ответственности: проблемы теории и правоприменительной практики // Вестник Московского университета МВД России. 2014. – № 8. –С. 87-94.

- меры общей превенции (например, политические, экономические, социальные, научно-технические, духовно-культурные)

- специальные превентивные меры (правовые, духовно-культурные, организационно-управленческие, технические, криминалистические и др.

Вместе с тем анализ настоящего параграфа диссертационного исследования позволяет сделать вывод, что повысить эффективность действующей на сегодняшний день в стране системы профилактики и предупреждения фактов мошенничества в сфере компьютерной информации можно путем разработки и внедрения в текущие процессы новых механизмов и методик деятельности государственных органов, в частности подразделений полиции и суда. Необходимо направить внимание на усовершенствование не только нормативной базы, регламентирующей вопросы мошенничества, ответственности за совершение этих деяний и способов взаимодействия в процессе разбирательств по делу органов государственной власти, но и на обеспечение высокого уровня технического оснащения правоохранительных органов.

2.3 Личность осужденных за мошенничество в сфере компьютерной информации

Как уже отмечалось, одной из главных причин появления и распространения преступлений в сфере компьютерной информации является повышение популярности среди населения интернет-деятельности и сформировавшегося в процессе использования информационных технологий доверия к ним со стороны граждан. Эти предпосылки стали причиной повышения значения интернета и компьютерной информации в жизни граждан, а, следовательно, определили интерес преступников к ценной

компьютерной информации, использование которой представляется для последних прибыльным видом деятельности.

Повышение уровня преступлений в сфере компьютерной информации неизбежно требует изучения обстоятельств их совершения и личности преступника. Благодаря установлению характерных особенностей личности кибер-преступников, органам следствия в процессе расследования по делу проще сформировать портрет преступника, обозначить подозреваемых в совершении деяния лиц и предположить варианты дальнейшего развития событий в деле.

Личность преступника представляет собой звено преступного механизма, которое грает важнейшую роль в этой системе. Характерные признаки личности преступника, которые выступают причиной преступного поведения, должны определяться государством, как цель деятельности по противодействию нарушениям закона. Именно поэтому проблематика личности преступника имеет большое значение в процессе анализа преступных посягательств и представляет собой один из сложных вопросов современной криминологии.

Исследование личности преступника признается одним из основных направлений криминологии. Изобличение преступников, совершающих преступления, в частности, в сфере компьютерной информации, в большинстве случаев возможно благодаря результатам научных исследований этого вопроса и изучению личности преступника правоприменителями. Этот криминологический элемент системы правонарушения называется специалистами главной причиной совершения противоправных действий, т.к. выступает аргументацией преступника при совершении им тех или иных противозаконных действий. Предупредительная деятельность законодателя должна осуществляться с учетом столь важного элемента, в частности, государство должно создавать

возможности корректировки негативных качеств преступников, их перевоспитание, изменение личности[58].

В криминологической науке принято изучать личность преступника исходя из особенностей преступного поведения. Целью такого исследования выступает определение первопричины, которая повлияла на формирование у субъекта антиобщественных установок и выявление социально-психологических признаков личности обвиняемого. В числе таких признаков рассматриваются различные категории характеристик: физические, социальные, коммуникативные, моральные, психические и т.п. Это обусловлено мнением, распространенным в юридической науке, согласно которому любое преступление берет начало в особенностях предшествующей его совершению жизни преступника, на мотив совершения оказывает влияние воспитание, обстоятельства жизни индивидуума, которые могли повлиять на принятый выбор образа жизни.

Лица, принимающие участие в организации или реализации мошенничества в области компьютерной информации, представляют различные категории населения. Это могут быть высококвалифицированные в сфере компьютерных технологий специалисты, а могут быть лица, разбирающиеся в компьютерах и технологиях достаточно поверхностно. Правонарушители этой категории различны по социальному статусу и по уровню поученного ими образования.

Важно отметить, что несмотря на актуальность решения проблемы преступности в сфере компьютерной информации и ее предупреждения, на сегодняшний день ни отечественные, ни зарубежные юристы не сформировали четкого портрета компьютерного мошенника.

Связи с чем предпримем попытку собственного определения личности осужденного, по ст. 159.6 УК РФ. Характеризуя личность преступника

---

[58] Кравцов И.А. К вопросу о социально–демографических признаках личности преступника, совершающего хищение чужого имущества с использованием служебного положения, на территории Центрально– Черноземного региона // Вестник ВИ МВД России. 2011.– № 3. С. 44.

обратимся к данным судебного департамента. За отчётный период 2020 года в 27 из 29 случаев мошенничество в сфере компьютерной информации было совершено мужчинами, что составляет 93, 1 % от удельного количества рассматриваемого преступления. Подавляющим количеством осужденных за преступление, предусмотренное ст. 159.6 УК РФ составляют преступники в возрасте от 18 до 24 в 2020 году их количество составило 12 человек, что составляет 41, 38% от общего числа осужденных, второй возрастной группой занимающей.

Абсолютное количество осужденных 29 были постоянным жителями местности совершение преступления, также абсолютно число осуждённых лиц по данному составу преступления являлись гражданами РФ. Преобладающим уровнем образования лиц, совершивших рассматриваемое преступления, являлось средне - профессиональное образование им обладали 14 осужденных – 48, 28 % от общего числа осужденных. Характеризуя род занятий, осужденных следует отметить, что 13 лиц, то есть 44, 83 % от общего числа осуждённых лиц являлись трудоспособными лицами без постоянного источника дохода

В 2019 году по анализируемой 159.6 статье УК РФ, всего осуждено было 134 лица, при этом 79 осужденных являлись мужчинами, их удельный вес по отношению к общему количеству осужденных составил 58, 9 %. Возраст осужденных в анализируемом году колебался. Возраст 2 осужденных составлял от 18-24 лет, 8 осужденных достигли возраста 25-29 лет, и подавляющему количеству осужденных 89, приходилось порядка 30 – 49 годам, их удельный вес по отношению к общему количеству осужденных составил 66, 42 %. Примечательно, что возраст 37 осужденных превышал 50 лет.

123 осужденных лица постоянно проживали в местности совершение преступлений, их удельный вес, их удельный вес по отношению к общему числу осужденных составил 97, 79 % при этом 13 лиц проживали в иной местности. Преобладающим уровнем образования осужденных являлось

высшее профессионально образование, количество лиц с данным уровнем образования в рассматриваемый период составляло 108 или 80, 6 % от общего числа. 21 осужденный имел среднее профессиональное образование, 7 лиц имело только среднее образование.

Примечательно, что в анализируемый период 97 осужденных являлись служащими коммерческой или иной организации, их удельный вес составил 72, 39%. Кроме того, 12 лиц являлись лицами, осуществляющими предпринимательскую деятельность. 7 лиц являлись трудоспособными без постоянного источника дохода, 6 выступали лицами прочих занятий и 2 лица являлись нетрудоспособными.

В 2018 году по анализируемой 159.6 статье УК РФ, всего осуждено было 54 лица, при этом 43 осужденных являлись мужчинами, их удельный вес по отношению к общему количеству осужденных составил 79, 63 %. Возраст осужденных в анализируемом году был сравнительно равным Возраст 20 осужденных составлял от 18-24 лет, их удельный вес по отношению к общему количеству осужденных составил 66, 42 %. 18 осужденным приходилось от 25-19 лет. 16 осужденным приходилось порядка 30 – 49 годам,

42 осужденных лица постоянно проживали в местности совершение преступлений, их удельный вес, их удельный вес по отношению к общему числу осужденных составил 77, 78 % при этом 12 лиц проживали в иной местности. Преобладающим уровнем образования осужденных являлось высшее профессионально образование, количество лиц с данным уровнем образования в рассматриваемый период составляло 17 или 31, 48 % от общего числа. 16 осужденный имел среднее профессиональное образование, 15 лиц имели среднее образование, кроме того 6 лиц имели только среднее общее, начальное образование или не имели образования.

Касательно рода занятости в анализируемый период 25 осужденных являлись трудоспособными без постоянного источника дохода, их удельный вес составил 46, 3%. Кроме того, 12 осужденных являлись служащими

коммерческой или иной организации. 11 лиц являлись рабочими, 2 лица являлись лицами, осуществляющими предпринимательскую деятельность. Примечательно, что 1 лицо входило в число иных сотрудников правоохранительных органов, в том числе органов прокуратуры. 1 лицо занималось иными занятиями[59].

Далее с целью установления индивидуальной и социально-психологической характеристики осужденного по ст. 159.6 УК РФ обратимся к материалам судебной практики.

Как правило в социальном отношении осужденные по рассматриваемому составу преступления характеризуются положительно «…Допрошенные в судебном заседании свидетели ФИО3, ФИО15, ФИО2 охарактеризовали подсудимого исключительно с положительной стороны, как заботливого сына, внука, брата, работающего, положительно характеризующегося…»[60]; «…социально адаптирован, имеет семью, положительно характеризуется по месту жительства, на учетах у нарколога и психиатра не состоит…»[61] лишь в одном случае судом было установлена отрицательная характеристика личности преступника : «…по месту проживания характеризуется отрицательно, не состоит в браке, не работает, имела инвалидность в детстве, состояла на учете в инспекции ПДН, состоит на учете наркологическом и психиатрическом диспансерах, лишена родительских прав в отношении малолетнего ребенка…»[62].

---

[59] Сводные статистические сведения о состоянии судимости в России [Электронный ресурс] // Судебный департамент при Верховном Суде РФ. - URL: https://xn--b1aew.xn--p1ai/reports/item/23816756/ (дата обращения 12.05.2021 г.)

[60] Приговор Хамовнического районного суда г. Москвы № 1-49/2014 от 15 мая 2014 года [Электронный ресурс] // Sud Praktika.ru. - URL: https://sud-praktika.ru/precedent/78293.html (дата обращения 13.05.2021 г.)

[61] Приговор Рудничного районного суда г. Кемерово Кемеровской области № 1-41/2017 от 31 января 2017 года [Электронный ресурс] // Sud Praktika.ru. - URL: https://sud-praktika.ru/precedent/342766.html (дата обращения 13.05.2021 г.)

[62] Приговор Рудничного районного суда г. Кемерово Кемеровской области № 1-336/2017 от 27 сентября 2017 года [Электронный ресурс] // Sud Praktika.ru. - URL: https://sud-praktika.ru/precedent/548118.html (дата обращения 13.05.2021 г.)

Индивидуально-психологическая характеристика осужденного характеризуется в абсолютном числе, проанализированном автором судебных решений деятельным раскаянием, добровольным возмещением вреда, способствованием в раскрытии преступлений, полным признанием вины подсудимого[63]. Однако вместе с тем практически в половине рассмотренных судебных решений, преступления осужденными были совершены в период непогашенной судимости[64][65].

Анализируя вышеизложенные статистические данные Судебного департамента ВС РФ, а также данные судебной практика попытаемся вывести усреднённый портрет личности осужденного, совершившего мошенничество по ст. 159.6 УК РФ.

Так типовой криминологический портрет личности российского мошенника в сфере компьютерной информации в настоящее время выглядит следующим образом: это мужчина в возрасте до 35 лет, проживающий в местности совершения преступления; имеющий среднее специальное или высшее профессиональное образование; не состоящий в семейном браке; безработный, либо служащий коммерческой или иной организации (более вероятно работающий специалист в области IT-технологий). В части социальных взаимоотношений характеризуется положительно, социально адаптирован, часто имеют семью; характеризуется деятельным раскаянием по отношению к совершенному преступлению, стремлением возместить причинённый ущерб, содействует в расследовании преступления.

---

[63] Приговор Ленинского районный суд г. Ульяновска № 1-89/2017 от 03 апреля 2017 года [Электронный ресурс] // Sud Praktika.ru. - URL: https://sud-praktika.ru/precedent/295713.html (дата обращения 13.05.2021 г.)

[64] Приговор Ленинского районного суда г. Екатеринбург №1-144/2017 от 20 марта 2017 года [Электронный ресурс] // Sud Praktika.ru. - URL: https://sud-praktika.ru/precedent/356488.html (дата обращения 13.05. 2021 г.)

[65] Приговор Рудничного районного суда г. Кемерово Кемеровской области № 1-44/2017 от 31 января 2017 года [Электронный ресурс] // Sud Praktika.ru. - URL: https://sud-praktika.ru/precedent/342763.html (дата обращения 13.05.2021 г.)

ЗАКЛЮЧЕНИЕ

Анализ проведенного исследования позволяет прийти к следующим выводам:

1. Мошенничество в сфере компьютерной информации является специальным видом мошенничества, которое также посягает на отношения собственности, но при этом совершается специфическими способами. Объектом данного правонарушения выступают отношения, посягающие на право собственности граждан или юридических лиц, дополнительный объект — правоотношения, обеспечивающие информационную безопасность. Объективная же сторона может быть выражена только в активных действиях, как на то указывает законодатель. В вопросе квалификации данного деяния большое значение имеют способы совершения подобного рода посягательства, к которым относятся: ввод, удаление, блокирование, модификация компьютерной информации или иное вмешательство, которое влечет за собой последствия в виде причинения ущерба субъектам права. Наиболее распространённым способом совершения преступления выступает

ввод удаление, блокирование, модификация компьютерной информации, лицами, имеющими доступ к базам данных, а также вмешательство с использованием вредоносных программ.

2. Субъект преступления, предусмотренного ст. 159.6 УК РФ общий. Привлечь к ответственности за совершение мошенничества в сфере компьютерной информации возможно физическое лицо, достигшее возраста шестнадцати лет и отвечающее критериям вменяемости, за исключением п. «а» ч. 3 с. 159.6 УК РФ, поскольку на основании данной нормы субъектом выступает лицо, использующее свое служебное положение в преступных целях. Субъективная сторона преступного посягательства предполагает умышленную форму вину и корыстную цель совершения преступления.

3. Основным преступлением, с которым смешивается мошенничество в сфере компьютерной информации, выступает неправомерный доступ к компьютерной информации. Об этом свидетельствуют и материалы судебной практики. Однако отграничивать данные посягательства между собой крайне важно – поскольку они имеют различный объект и соответственно различную степень общественной безопасности, что в конечном итоге отражается на применяемой по отношению к виновной санкции.

Кроме того, согласно разъяснениям Пленума ВС РФ действия виновного, должны быть расценены не только по ст. 159.6 УК РФ, но также и по соответствующей норме главы 28 УК РФ.

4. Состояния преступления, связанных с мошенничества в сфере компьютерной информации, характеризуется сравнительно небольшим удельным весом, по отношению к остальным зарегистрированных преступлений, а также в количестве зарегистрированных преступлений на 100 тыс. жителей. Тем не менее мошенничество в сфере компьютерной информации характеризуется высокой латентностью и сложностью расследования отчего сравнительно невысокое количество регистрируемых преступлений не свидетельствует о низкой опасности рассматриваемого вида преступления.

5. Структура мошенничества в сфере компьютерной информации характеризуется также сравнительно низким удельным весом по отношению к общему числу зарегистрированных преступлений, общему составу мошенничеству и смежным видам преступлений в сфере компьютерной информации. Данные о лицах, совершивших преступление характеризуются преобладанием мужчин, как субъектов преступления. Возраст преступников в преобладающем количестве составлял от 18-24 лет, преобладающим уровнем образование выступило средне профессиональное. Преступления в абсолютном количестве случае совершалось в постоянном месте проживания преступника, также в подавляющем количестве осужденные являлись трудоспособными лицами без постоянного источника дохода.

6. Динамика мошенничества в сфере компьютерной информации характеризуется сравнительно стабильным приростом регистрируемых преступлений, средний показатель темпа прироста за анализируемый период составил порядка 10%.

7. Меры предупреждение мошенничества в сфере компьютерной информации классифицируются на:

- меры общей превенции (например, политические, экономические, социальные, научно-технические, духовно-культурные)

- специальные превентивные меры (правовые, духовно-культурные, организационно-управленческие, технические, криминалистические и др.

Вместе с тем анализ проведенного исследования позволяет следует вывод, что повысить эффективность действующей на сегодняшний день в стране системы профилактики и предупреждения фактов мошенничества в сфере компьютерной информации можно путем разработки и внедрения в текущие процессы новых механизмов и методик деятельности государственных органов, в частности подразделений полиции и суда. Необходимо направить внимание на усовершенствование не только нормативной базы, регламентирующей вопросы мошенничества, ответственности за совершение этих деяний и способов взаимодействия в

процессе разбирательств по делу органов государственной власти, но и на обеспечение высокого уровня технического оснащения правоохранительных органов.

8. Типовой криминологический портрет личности российского мошенника в сфере компьютерной информации в настоящее время выглядит следующим образом: это мужчина в возрасте до 35 лет, проживающий в местности совершения преступления; имеющий среднее специальное или высшее профессиональное образование; не состоящий в семейном браке; безработный, либо служащий коммерческой или иной организации (более вероятно работающий специалист в области IT-технологий). В части социальных взаимоотношений характеризуется положительно, социально адаптирован, часто имеют семью; характеризуется деятельным раскаянием по отношению к совершенному преступлению, стремлением возместить причинённый ущерб, содействует в расследовании преступления.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Уголовный кодекс Российской Федерации: федер. закон от 13 июня 1996 г. N 63-ФЗ: (ред. от 05 апреля 2021г., с изм. от 08 апреля 2021 г.)// КонсультантПлюс: справ. правовая система. Версия Проф. М., 2020. Режим доступа: локальная сеть Науч. б-ки Том. гос. ун-та.

2. Уголовно-процессуальный кодекс Российской Федерации: федер. закон от 18 декабря 2001г. N 174-ФЗ: (ред. от 05 апреля 2021г., с изм. От 13 апреля 2021 г.)// КонсультантПлюс: справ. правовая система. – Версия Проф. – Электрон. дан. - М., 1998. – Доступ из локальной сети Науч. б-ки Том. гос. ун-та.

3. Гражданский кодекс Российской Федерации (часть первая): федер. закон от 30 нояб. 1994 г. № 51-ФЗ: (ред. от 31 июля. 2020 г.) // КонсультантПлюс: справ. правовая система. − Версия Проф. − М., 2020. – Режим доступа: локальная сеть Науч. б-ки Том. гос. ун-та.

4. Федеральный закон от 27 июня 2011 г. N 161-ФЗ (ред. от 22 декабря 2020 г.) «О национальной платежной системе" (с изм. и доп., вступ. в

силу с 01 января 2021 г.) // КонсультантПлюс: справ. правовая система. − Версия Проф. − М., 2020. – Режим доступа: локальная сеть Науч. б-ки Том. гос. ун-та.

5. Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31 июля 2020 г. N 259-ФЗ // КонсультантПлюс: справ. правовая система. Версия Проф. М., 2020. Режим доступа: локальная сеть Науч. б-ки Том. гос. ун-та.

6. Барчуков В. К. К вопросу о содержании признаков объективной стороны мошенничества в сфере компьютерной информации // Безопасность бизнеса. – 2016. – № 5. – С. 41–46.

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

8. Гарбатович Д.А. Проблемные аспекты эффективности норм, предусматривающих ответственность за совершение преступлений в сфере компьютерной информации // Библиотека криминалиста. – 2013. – № 5. – С. 6-14.

9. Гладких В.И. Компьютерное мошенничество: а были ли основания для криминализации? // Рос. следователь. – 2014. – № 22. – С. 25-31.

10. Грунтов И.О. К вопросу о понимании объекта преступления в уголовном праве /И.О. Грунтов // Труд. Работа. Профсоюз. Общество. – 2017. – № 2(56). – С. 41 – 46.

11. Дворецкий М. Ю. Уголовная ответственность за мошенничество в сфере компьютерной информации: проблемы теории и правоприменительной практики // Вестник ТГУ. 2013. №8 (124). С. 407 – 410.

12. Дворецкий М.Ю., Стромов В.Ю. Эффективная реализация уголовной ответственности: проблемы теории и правоприменительной

практики // Вестник Московского университета МВД России. 2014. – № 8. – С. 87-94.

13. Егорова М. А., Кожевина О. В. Место криптовалюты в системе объектов гражданских прав // Актуальные проблемы российского права. — 2020. — Т. 15. — № 1. — С. 81—91.

14. Зинина У. В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: автореф. дис. ... канд. юрид. наук, М., 2007. – 34 с.

15. Иващенко Н.Д. Мошенничество в сфере компьютерной информации: проблемные вопросы // Столица науки. 2020. № 6. С. 269-276.

16. Иногамова-Хегай Л. В. Мошенничество, присвоение, растрата: проблемы квалификации конкурирующих и смежных норм // Уголовное право. 2015. №5. С. 30 – 34.

17. Капитализация криптовалют впервые превысила $ 2 трлн [Электронный ресурс] // Телеканал «РБК». URL: https://www.rbc.ru/crypto/news/606b2d0a9a794773b0013395 (дата обращения 19.05.2021 г.)

18. Кленова Т.В. О разграничении смежных и конкурирующих составов преступлений (на примере мошенничества) [Электронный ресурс] // Предпринимательство и право. – URL: http://lexandbusiness.ru/view-article.php?id=2359 (дата обращения 19.05.2021 г.)

19. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. М.: Горячая линия–Телком, 2002. – 336 с.

20. Коростелев М. А. Правовой режим электронных денег в гражданском законодательстве: автореф. дис. . канд. юрид. наук. М., 2015. – 36 с.

21. Кравцов И.А. К вопросу о социально–демографических признаках личности преступника, совершающего хищение чужого имущества с использованием служебного положения, на территории Центрально– Черноземного региона // Вестник ВИ МВД России. 2011.– № 3. С. 43-47.

22. Кропачев С.Ю. Мошенничество в сфере компьютерной информации как угроза экономической деятельности: актуальные вопросы квалификации // Современная наука: актуальные проблемы теории и практики. серия: экономика и право. 2020. № 4. С. 183 – 187.

23. Кулешова Н. Н., Христофорова Е. И. Особенности квалификации мошенничества в сфере компьютерной информации // Вопросы науки и образования. 2018. № 14 (26). С. 41-46.

24. Куликов А.В., Гуц Е.А. Мошенничество в сфере компьютерной информации // Известия тульского государственного университета. экономические и юридические науки. 2020. № 1. С. 81 - 88.

25. Курс мировой и российской криминологии в 2 т. Т. II. Особенная часть: учебник для вузов / В. В. Лунеев. — М.: Издательство Юрайт, 2015. — 872 с. — Серия: Магистр.

26. Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: дис. ... д-ра юрид. наук / Т.М. Лопатина. — М.: РГБ, 2007. — 418. с

27. Лопатина Т. М. Проблемы уголовно- правовой защиты сфер компьютерной информации: современный взгляд на мошенничество // Право и безопасность. 2013. №3-4 (45). С. 98 – 95

28. Ляпунов Ю.И., Пушкин А.В. Преступления в сфере компьютерной информации. Уголовное право. Особенная часть [Текст] / Под ред. Н.И. Ветрова, Ю.И. Ляпунова. – М., 2016. – 866 с.

29. Медведев С. С. Мошенничество в сфере высоких технологий: автореф. дис. .канд. юрид. наук . Краснодар, 2008. – 22 с.

30. Новости ООН [Электронный ресурс] - URL: https://news.un.org/ru/story/2015/05/1263871#.VY5a1psdCt8 (дата обращения: 12.05.2021).

31. Прозументов Л. М., Шеслер А.В. Криминология. Общая часть: Учебник. – Томск: ООО «ДиВо», 2007. – 230 с.

32. Подольный Н.А. Отдельные проблемы расследования преступлений, совершённых с применением компьютерных технологий // Библиотека криминалиста. – 2013. -№ 5. – С. 116- 127.

33. Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате». № 48 // КонсультантПлюс: справ. правовая система. Версия Проф. М., 2020. Режим доступа: локальная сеть Науч. б-ки Том. гос. ун-та.

34. 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. – 222 с.

35. Сводные статистические сведения о состоянии судимости в России [Электронный ресурс] // Судебный департамент при Верховном Суде РФ. - URL: https://xn--b1aew.xn--p1ai/reports/item/23816756/ (дата обращения 12.05.2021 г.)

36. Статистические сведения о состоянии преступности [Электронный ресурс] // Министерство внутренних дел РФ. - URL: https://xn--b1aew.xn--p1ai/reports/item/23816756/ (дата обращения 12.05.2021 г.)

37. Степанов М.В. Критический анализ нормы о мошенничестве в сфере компьютерной информации (ст. 159.6 УК РФ) // Юридическая наука и практика: Вестник Нижегородского академии МВД России. 2016. № 1. 174. С. 85 – 88.

38. Степанова К.В. Мошенничество в сфере компьютерной информации: российский и зарубежный опыт // Актуальные проблемы уголовного права, уголовного процесса и криминалистики. 2019. С. 32-38.

39. Уголовное право России. Общая часть: учебник для академического бакалавра/ под ред. О.С. Капинус. – М. Издательство Юрайт, 2015. Серия: Бакалавр. Академический курс. – 539 с.

40. Фомин С. А. Криминологические характеристики преступности и основные показатели характеристик преступности, ее отдельных групп и

видов на современном этапе // Вестник Сибирского юридического института МВД России. 2018. №1 (30) С. 94 – 103.

41. Чучаев, А.И Комментарий к Уголовному кодексу Российской Федерации (постатейный) /А.И. Чучаев М.: Норма, 2015. – 71 с.

42. Щедрин Н.В. Основы общей теории предупреждения преступности: Учеб. пособие / Краснояр. гос. ун-т, 1999. - 58 с.

Приложение А. Динамика мошенничества в сфере компьютерной информации по данным МВД РФ

Таблица А.1 Зарегистрировано преступлений, предусмотренных ст. 159.6 в России

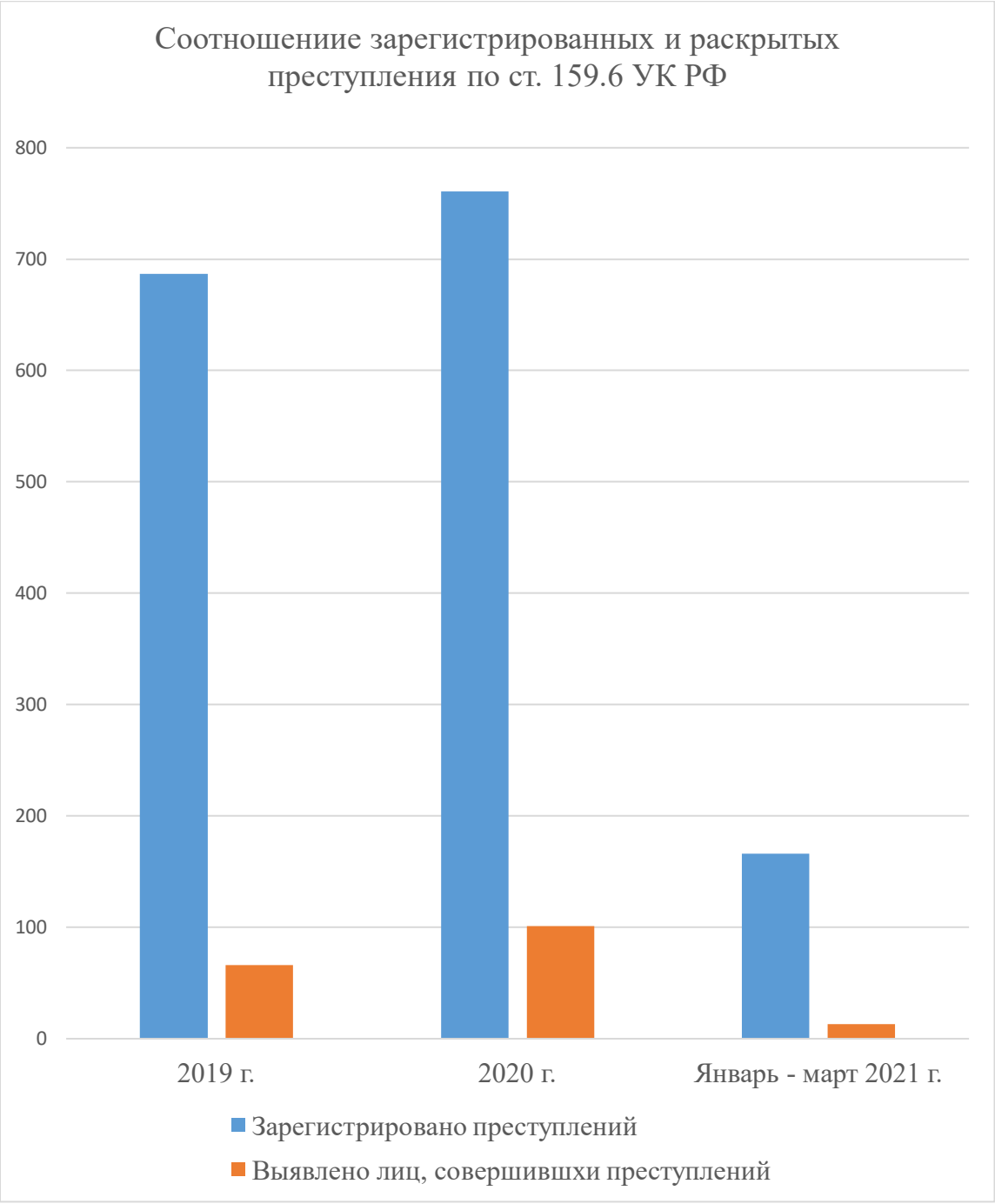
Годы	Всего	Прирост (снижение) в % к предыдущему году)
2019 г.	687	- 29, 2
2020 г.	761	10, 8

Таблица А.2 Выявлено лиц, совершивших преступления, предусмотренные ст. 159.6 в России

Годы	Всего	Прирост (снижение) в % к предыдущему году)
2019 г.	66	- 46, 3
2020 г.	101	53, 0

Приложение Б. Соотношение зарегистрированных и раскрытых преступлений по ст. 159.6 УК РФ по данным МВД РФ

Рисунок Б.1 Соотношение зарегистрированных и раскрытых преступления по ст. 159.6 УК РФ



Приложение В. Структура мошенничества в сфере компьютерной информации по данным МВД РФ

Рисунок В.1 Удельный вес мошенничества в сфере компьютерной информации по отношению к общему составу мошенничества

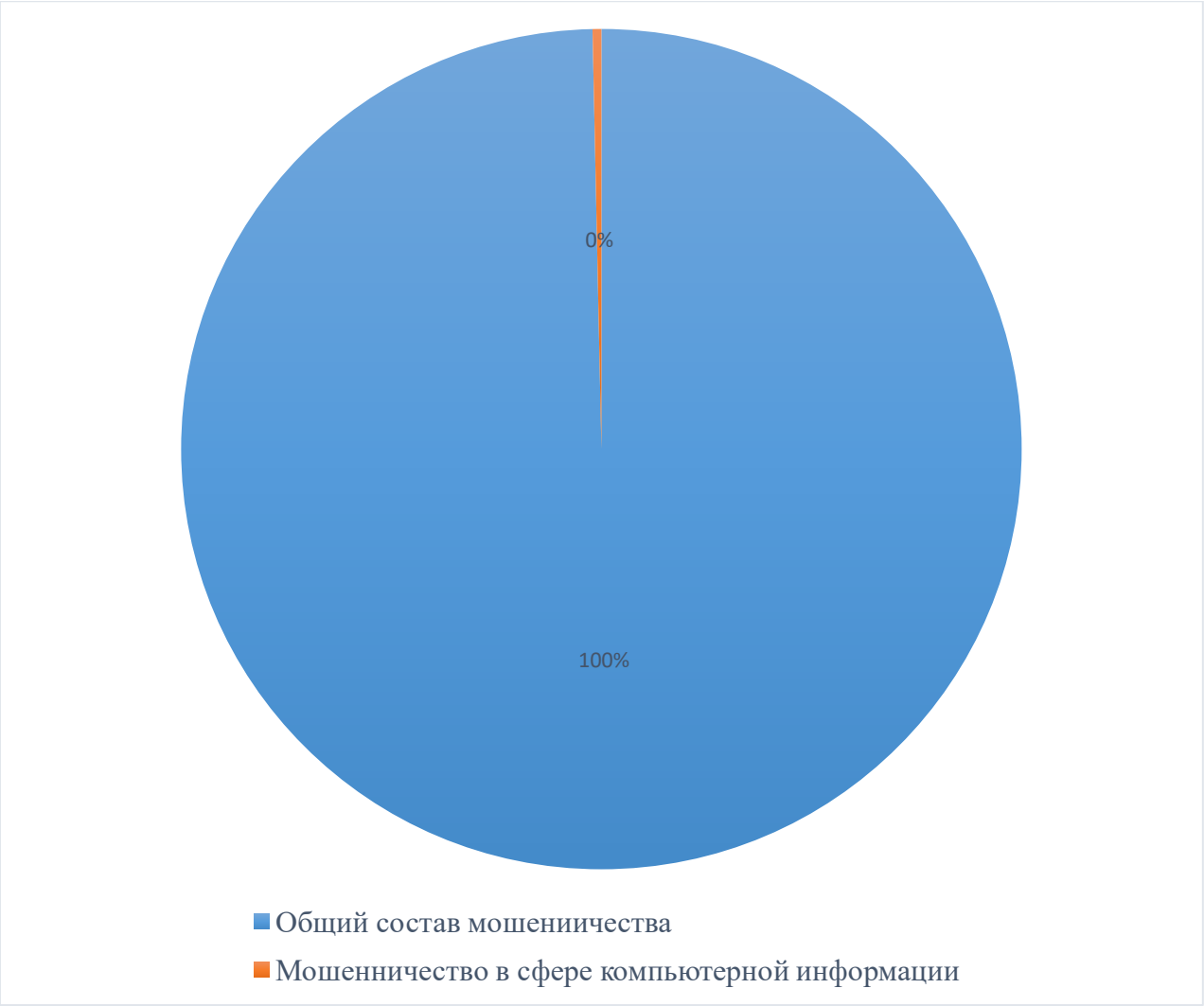
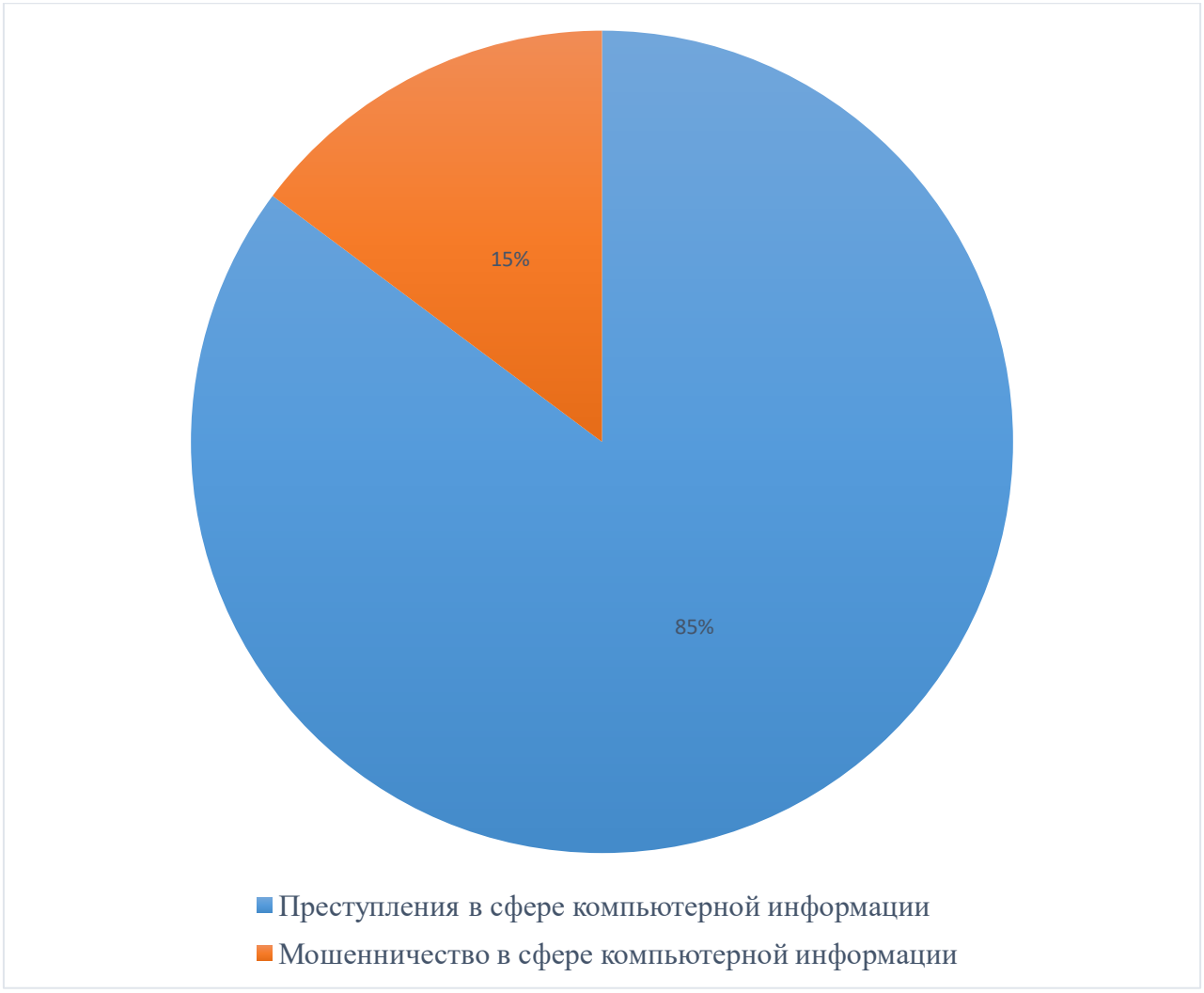


Рисунок В.2 Удельный вес мошенничества в сфере компьютерной информации по отношению к смежным составам преступлений


15%
85%
Преступления в сфере компьютерной информации
Мошенничество в сфере компьютерной информации