Министерство внутренних дел Российской Федерации
Федеральное государственное казенное образовательное учреждение высшего образования «Казанский юридический институт Министерства внутренних дел Российской Федерации»

Кафедра: Уголовного права

ДИПЛОМНАЯ РАБОТА

На тему: Уголовная ответственность за мошенничество в сфере компьютерной информации

Выполнил:
слушатель 5 курса 092 уч. гр.,
специальность 40.05.02
Правоохранительная деятельность,
2019 года набора,
Ялалов Данил Ильмирович

Руководитель:
кандидат социологических наук,
старший преподаватель кафедры
уголовного права
подполковник полиции
Нурутдинов Ильнур Ильдусович

Рецензент:
ВРИО заместителя начальника
ОП №4 «Электротехнический»
УМВД России
по г. Набережные Челны
подполковник полиции
Идиятуллин Руслан Растямович

Дата защиты: «__»_____2024г. Оценка_____

Казань 2024

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. Компьютеризация ознаменовала новую эпоху научно – технического прогресса. Все новейшие изобретения создавались с целью упростить жизнь человека в современном обществе, сделать его наиболее мобильным и оперативным. Но, как известно, у каждого прогресса есть как положительные стороны, так и отрицательные. В данном случае, это появление нового вида противоправных деяний, преступлений в сфере компьютерной информации. Данный вид противоправного деяния имеет свою специфику, как по механизму его совершения, так и по его способам. Однако, преступления в сфере компьютерной информации характеризуются большой латентностью и низкой раскрываемостью, что способствует увеличению количества деяний и совершенствование навыков лиц их совершающих.

Все больше и больше данных содержится и обрабатывается в компьютерных информационных системах. Применение компьютерных технологий в целях обработки и обмена данными между различными пользователями информационного пространства практически во всех сферах жизни общества является положительным моментом, соответствующим требованиям времени. В данном контексте возникает две точки зрения: первая – информационное пространство и компьютерные технологии дают возможность совершенствовать социально-экономические процессы на современном этапе развития общества в процессе цифровизации; вторая – появилась киберпреступность.

В настоящее время уголовное законодательство предусматривает ответственность за мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств

хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей (ст. 159.6 Уголовного кодекса РФ (далее – УК РФ)). Данная статья была введена Федеральным законом от 29.11.2021 №207.

Согласно статистическим данным, за 2019-2023 гг. было зарегистрировано следующее количество преступлений, предусмотренных ст. 159.6 УК РФ:

1) 2019 – 687;

2) 2020 – 761;

3) 2021 – 431;

4) 2022 – 334;

5) 2023 – 417[1].

Кроме того, за 2022 год по ч. 2 ст. 159.6 УК РФ было осуждено 5 человека: с видом наказания в виде лишения свободы условно – 4, 1 – штрафа, по ч. 3 ст. 159.6 УК РФ – 8, лишение свободы условно – 6, штраф – 2; ч. 4 ст. 159.6 УК РФ – 16: лишение свободы – 10, лишение свободы условно – 6[2].

Следует отметить, что уменьшение количества зарегистрированных преступлений, предусмотренных ст. 159.6 УК РФ не говорит об уменьшении уровни исследуемого вида преступления, а наоборот: у сотрудников правоохранительных органов возникают трудности при выявлении исследуемых видов преступлений, что отражается на статистических данных о преступлениях, зарегистрированных на территории Российской Федерации.

Целью настоящей работы является комплексное исследование особенностей назначения уголовной ответственности за мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ).

Задачами настоящей работы выступают:

---

[1] Состояние преступности на территории Российской Федерации. URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 10.01.2024).

[2] Состояние преступности на территории Российской Федерации. URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 10.01.2024).

1. Анализ объективных признаков мошенничества в сфере компьютерной информации.

2. Исследование субъективные признаки мошенничества в сфере компьютерной информации.

3. Рассмотрение актуальных вопросов разграничения мошенничества в сфере компьютерной информации от иных смежных составов.

4. Изучение особенностей назначения наказания за совершение мошенничества в сфере компьютерной информации.

Объект настоящего исследования – общественные отношения, возникающие при квалификации совершенных противоправных деяний, подпадающих под признаки состава преступлений, предусмотренных ст. 159.6 УК РФ.

Предмет настоящего исследования – нормы, регламентирующие уголовную ответственность и наказание за совершение противоправных деяний, подпадающих под признаки состава преступлений, предусмотренных ст. 159.6 УК РФ.

Методологическая основа исследования включает в себя систему идей научного познания, а именно: универсально-металогический диалектический метод и структурно-системный подход; общенаучные (анализ, синтез, индукция, дедукция, сравнение, общение) и частнонаучные (уголовно-статистический, изучение нормативно-правовых актов, анализ практического опыта) методы познания.

Эмпирическая основа включает в себя: материалы правоприменительной практики, статистические данные Министерства внутренних дел Российской Федерации, Генеральной прокуратуры Российской Федерации, Судебного департамента при Верховном суде Российской Федерации и иных правоохранительных органов; социологические, криминологические и криминалистические исследования ученых.

Различными аспектами исследования проблем, возникающих при назначения уголовной ответственности за мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) занимались такие авторы, как: Т.В. Абдульмянова, Г. Адашевский, Д.С. Алексеев, Е.В. Алферова, И.П. Асанова, Е.Н. Бархатова, С.Я. Бойко, А.В. Борисов, В.Б. Боровиков, А.В. Бородин, В.А. Власов, В.В. Данилов, В.В. Коломинов, В.А. Кондратова, А.В. Куликов, Н.А. Лопашенко, А.О. Миронов, И.В. Морозова, Е.И. Рождайкина, И.В. Савельев, В.В. Сверчков, М.В. Степанов, З.И. Хисамова, А.А. Энгельгардт и др.

Работа состоит из введения, двух глав, включающих в себя четыре параграфа, заключения, списка использованной литературы.

Теоретическая и практическая значимость работы заключается в том, что результаты проведенного исследования могут быть использованы в дальнейших научных разработках автора дипломной работы, в образовательной деятельности при преподавании соответствующих учебных курсов по теме исследования, при разработке учебно-методических материалов и пособий, а также в профессиональной деятельности сотрудников правоохранительных органов.

Краткая характеристика основных положений дипломной работы. Структура дипломной работы состоит из следующих элементов: введения, двух глав, четырех параграфов, заключения и списка использованной литературы. Первая глава работы посвящена исследованию объективных и субъективных признаков ст. 159.6 УК РФ, указаны особенности признаков данного преступления. Во второй главе проанализированы особенности установления признаков преступления, регламентированного ст. 159.6 УК РФ, обозначены наказания за совершения мошенничества в сфере компьютерной информации. В работе представлены способы совершения преступления, предусмотренного ст. 159.6 УК РФ. В заключении представлены выводы по теме исследования. В списке используемой литературе указаны источники, используемые в ходе написания работы.

ГЛАВА 1. УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

§ 1. Объективные признаки мошенничества в сфере компьютерной информации

Квалификация мошенничества по вышеназванным статьям УК РФ зависит, в первую очередь, от той сферы общественных отношений, в которой совершается данной преступление, а также от предмета преступного посягательства и способа совершения преступного деяния (критерии выделения специальных составов мошенничества).

В науке уголовного права деяние, предусмотренное ст. 159 УК РФ принято называть «простым» мошенничеством. Объективные и субъективные признаки данного вида мошенничества будут рассмотрены в следующей главе. В рамках данного параграфа необходимо определить сущность специальных видов мошенничества, а также степень их распространенности в общей структуре преступности.

В уголовном праве к объективным признакам любого преступного деяния относятся его объект и объективная сторона. Традиционно, под «объектом преступления» понимают общественные отношения, взятые под охрану уголовным законодательством[1].

Родовой объект мошенничества, как и других преступных деяний, как правило, совпадает с наименованием раздела Уголовного закона, в который включена соответствующая статья – Раздел VIII. Преступления в сфере экономики. По мнению А.В. Борисова, «родовой объект составляют

[1] Уголовное право. Особенная часть : учебник для вузов / А. В. Наумов [и др.] ; ответственные редакторы А. В. Наумов, А. Г. Кибальник. – 5-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2023. – 499 с.

общественные отношения в сфере экономики, которые состоят, исходя из содержания раздела VIII УК РФ, из отношений собственности, отношений, связанных с организацией производственных процессов, организационно-экономических отношений, а также возникающих в ходе их становления и развития социально-экономических связей»[1].

Видовой объект определяется главой Уголовного закона, в которой содержится конкретная статья, в данном случае ст. 159.6 УК РФ – глава 21. Преступления против собственности. Согласно мнению А.В. Борисова, «видовой и непосредственный объекты мошенничества совпадают, их составляют интересы собственности».

Объект анализируемого преступления полностью совпадает с родовым объектом хищения – это общественные отношения, сложившиеся в сфере электронного документооборота. Как и мошенничество вообще, квалифицированное мошенничество в сфере компьютерных технологий – всегда хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

При рассмотрение объективной стороны особое внимание хотелось бы обратить внимание на способ совершения преступления. Объективная сторона мошенничества по ст. 159 УК РФ выражается в противоправном завладении чужого имущества путем обмана или злоупотребления доверия, с целью обращения имущества в свои пользу или ползу третьи лиц. Такое содержание объективной стороны прослеживается в ст.159-159.5 УК РФ, однако в ст. 159.6 УК РФ объективная сторона выражается в доступе к компьютерной системе путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств

[1] Борисов, А. В. О некоторых аспектах объекта мошенничества / А. В. Борисов // Военное право. – 2021. – № 4(68). – С. 264-269.

хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей[1].

Объективная сторона мошенничества в сфере компьютерной информации отличается собственной уникальностью. Законодатель, сохранив мошеннические формы (хищение и приобретение права на чужое имущество), исключил традиционные способы совершения деяния (обман, злоупотребление доверием). Вместо них объективная сторона характеризуются следующими способами: 1) ввод, удаление, блокирование, модификация компьютерной информации либо; 2) иное вмешательство в информационную сеть или информационно-телекоммуникационную сеть[2].

Под вводом компьютерной информации следует понимать введение (установку) в электронную память компьютера, иных устройств, способных выполнять функции приема, переработки, хранения и выдачи информации в электронном виде, в том числе мобильных телефонов, смартфонов, бортовых компьютеров транспортных средств, контрольно-кассовых машин, банкоматов и т.п., данных, необходимых для выполнения компьютерной программы, или программ самих по себе[3].

Под удалением (уничтожением) информации следует понимать приведение информации или ее части в непригодное для использования состояние, при котором исключается ее получение с соответствующего раздела памяти компьютера, иного устройства, съемного носителя или

---

[1] Рождайкина, Е. И. Особенности квалификации объекта и объективной стороны мошенничества в сфере компьютерной информации / Е. И. Рождайкина // Эволюция российского права : Материалы XIX Международной научной конференции молодых ученых и студентов, Екатеринбург, 29–30 апреля 2021 года / Уральский государственный юридический университет. – Екатеринбург: Федеральное государственное бюджетное образовательное учреждение высшего образования "Уральский государственный юридический университет", 2021. – С. 1276-1280.

[2] Степанов М. В. Критический анализ нормы о мошенничестве в сфере компьютерной информации (ст. 159.6 УК РФ). // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2019. – № 1 (33). – С. 173.

[3] Боровиков, В. Б. Уголовное право. Особенная часть : учебник для среднего профессионального образования / В. Б. Боровиков, А. А. Смердов ; под редакцией В. Б. Боровикова. – 7-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2023. – 505 с.

интернет-сайта, независимо от возможности восстановления данной информации. Не является уничтожением информации переименование файла, где она содержится, а также автоматическая замена обновленного файла.

Блокирование информации есть временное или постоянное ограничение либо фактическое закрытие доступа к ней, характеризующееся невозможностью использования информации по прямому назначению полностью или в требуемом режиме, однако не соединенное с ее (удалением) уничтожением.

При модификации происходит изменение содержания информации, затрудняющее восприятие ее в первоначальном виде. Не образует модификации изменение информации, которое не приводит к искажению ее смыслового содержания, например изменение шрифта, начертания, размера текста.

Под вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей надо понимать неправомерные действия, нарушающие процесс обработки, хранения, использования, передачи и иного обращения с компьютерной информацией, установленный Федеральным законом «Об информации, информационных технологиях и о защите информации» и другими нормативными правовыми актами.

Согласно материалам дела З.С.Е., посредством имеющегося у него компьютера, используя ранее найденную им банковскую карту ПАО «Сбербанк России» и мобильный телефон, принадлежащие К.Ю.Л., не имея каких-либо законных оснований, используя информационную компьютерную сеть «Интернет», услугу «Мобильный банк», путем ввода данных карты К.Ю.Л., оплатил заказанные ранее им товары, приобретенные в интернет – магазине «ДНС», списав с лицевого счета К.Ю.Л., денежные средства в

размере 17096,00 руб., которые перевел в счет оплаты товаров, причинив потерпевшему значительный материальный ущерб[1].

Изначально действия обвиняемого квалифицировали по ст. 159.6 УК РФ. Но в ходе дальнейшего судебного разбирательства обвинитель попросил переквалифицировать содеянное на п. «в» ч. 2 ст. 158 УК РФ мотивируя это тем, что обвиняемый не осуществлял мошеннических действий, и не было оказано воздействия на компьютерное обеспечение, то есть преступник не осуществлял действий, предусмотренных объективной стороной статьи 159.6. УК РФ.

Другой пример из практики Петрозаводского городского суда Республики Карелия. Обвинитель обратился в суд с требованиями о признании сайтов в информационно-коммуникационной сети «Интернет» информацией, распространение которой в Российской Федерации запрещено. В ходе рассмотрения обращения установлено, что на спорных сайтах, размещена информация с предложением по получению незаконного доступа к компьютерной информации (ддос услуги, продажа чужих аккаунтов социальных сетей, вредоносные компьютерные программы). Суд квалифицировал содеянное по ст. 159.6 УК РФ. Отметим, что ст. 159.6 УК РФ предусматривает уголовную ответственность за хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей[2].

---

[1] Приговор суда по ч. 2 ст. 159.6 УК РФ № 1-417/2017. URL: https://sud-praktika.ru/precedent/(дата обращения: 07.10.2023).

[2] Решение № 2А-7195/2020 2А-7195/2020~М-7803/2020 от 19 ноября 2020 г. по делу № 2А-7195/2020. URL: https://sudact.ru/regular/doc/ (дата обращения: 07.10.2023).

Согласно материалам правоприменительной практики по уголовным делам, предусмотренных ст. 159.6 УК РФ, выделяются несколько способов преступных действий:

1) взлом с последующим хищением данных;

2) оформление банковских карт с применением краденных данных жертвы;

3) кремминг;

4) «инвестиционные копилки»;

5) покупка акций по минимальной цене и распространение заведомо ложные сведения о юридическом лице через информационное пространство для создания большого спроса на них, ссылаясь на обладание секретной информацией о важном корпоративном событии;

6) использование электронных платежных средств (WebMoney, Яндекс.Деньги, Assist, Robox, Qiwi и др.);

7) спуффинг-атаки[1];

8) псевдоблаготворительность.

Более типичным способом совершения данного рода деяний является совершение преступления путем использования установленного на устройство потерпевшего вредоносного программного обеспечения. Так, в частности, Советским районным судом города Томска К.Р., Г.К. и Г.С. были осуждены за совершение ряда деяний при следующих обстоятельствах. На смартфоны потерпевших устанавливалось вредоносное программное обеспечение, позволяющее отправлять SMS-сообщения без ведома пользователя. С помощью данной программы производилась отправка сообщений, являвшихся, по сути, командами для перевода денежных средств на счет, заранее открытый на подставное лицо. Органами предварительного расследования деяние было квалифицировано как кража (ст. 158 УК РФ),

[1] Коломинов В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дис. … канд. юрид. наук. – Иркутск, 2017. – С. 12.

однако суд переквалифицировал его на мошенничество в сфере компьютерной информации. Суд апелляционной инстанции подтвердил выводы суда первой инстанции, правомерно указав, что, несмотря на отсутствие в обвинительном заключении слов «ввод», «модификация», «блокирование» компьютерной информации, в описании действий злоумышленников данные понятия были, по сути, раскрыты[1].

Данное решение суда следует признать правильным. Так, например, использование вредоносного функционала программного обеспечения по отправке SMS-сообщений без ведома пользователя (даже если оно по незнанию было загружено самим добросовестным пользователем), является вводом определенной информации; в свою очередь действия данной программы по удалению отправленных сообщений с целью сокрытия своей деятельности от пользователя являются, со всей очевидностью, уничтожением компьютерной информации. Таким образом, следует согласиться с решениями судов, правильно квалифицировавших деяние как мошенничество в сфере компьютерной информации. В то же время, следует отметить, что отдельные правоприменители неохотно квалифицируют деяние по указанной статье, склоняясь больше к «традиционным» составам хищений, таким, как кража и классическое мошенничество[2].

Представляется также, что именно по ст. 159.6 УК РФ следует квалифицировать деяния, связанные с использованием «троянцев-вымогателей», которые либо блокируют экран устройства, либо шифруют файлы пользователя с целью последующего требования выкупа. В данном случае способом совершения преступления будет являться блокирование компьютерной информации; возможное отсутствие обмана или злоупотребления не будет являться помехой, поскольку, как уже говорилось

---

[1] Апелляционное определение Томского областного суда от 12.10.2017 по делу № 22-1652/2017 // Справ.-правовая система «Консультант Плюс» (дата обращения: 07.10.2023).

[2] Сверчков, В. В. Уголовное право. Общая и Особенная части : учебник для вузов / В. В. Сверчков. – 10-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2023. – 727 с.

ранее, мошенничество в сфере компьютерной информации является особым видом хищения. Кроме того, в данном случае возможна дополнительная квалификация по ст. 273 УК РФ, поскольку создание вредоносного программного обеспечения само по себе не входит в описание способа совершения деяния, предусмотренного ст. 159.6 УК РФ[1].

Если первая группа действий связана с непосредственным воздействием на компьютерную информацию, то вторая направленна на источники ее хранения. Так, законодатель не раскрывает, что конкретно он понимает под таким действием, как «иное вмешательство». Представляется что под этими действиями следует понимать любое воспрепятствование нормальному процессу функционирования информационной или информационно-телекоммуникационной сети[2].

Под информацией, в соответствии с положениями действующего российского законодательства следует понимать «сведения (сообщения, данные) независимо от формы их представления» , в связи с чем полагаем необходимым уточнить термин и употреблять не «компьютерная информация», а «электронная информация», поскольку компьютер – не единственное электронное устройство, которое может воспринимать данную информацию[3].

Как уже отмечалось, своеобразие мошенничества в отличие от других форм хищений, предусмотренных гл. 21 УК РФ, состоит в том, что под влиянием обмана или злоупотребления доверием, потерпевший сам передаст свое имущество виновному. Соответственно, так или иначе, должен присутствовать потерпевший, в отношении которого производится обман или

---

[1] Куликов, А. В. Мошенничество в сфере компьютерной информации / А. В. Куликов, Е. А. Гуц // Известия Тульского государственного университета. Экономические и юридические науки. – 2020. – № 1. – С. 81-88.

[2] Энгельгардт А.А. Вопросы квалификации мошенничества в сфере компьютерной информации. // Право. Журнал Высшей школы экономики. – 2020. – № 4. – С. 86.

[3] Бородин, А. В. Объективная сторона мошенничества, предусмотренного статьей 159.6 уголовного кодекса Российской Федерации / А. В. Бородин, М. В. Косолапов // Colloquium-Journal. – 2019. – № 16-7(40). – С. 25-26.

которого вводят в заблуждение. Если же проанализировать существующую трактовку мошенничества в сфере компьютерной информации, то можно заметить, что там нет потерпевшего, как физического лица, а обман происходит по отношению к какой-либо банковской или кредитно-финансовой, или иной системы.

Так, например, в приговоре Первомайского районного суда г. Владивостока указывается, что обвиняемый С. приобрел сим-карту, номер которой был привязан к Мобильному банку предыдущего владельца, что позволило ему перевести на собственный счет через смс-сообщение денежную сумму в размере 10 000 (десяти тысяч) рублей, о чем потрепавший и не догадывался. Его действия были квалифицированы судом по ч. 2 ст. 159.6 УК РФ[1].

Еще одна проблема заключается в конкуренции ст. 159.3 и 159.6 УК РФ в ситуациях, когда посредством использования электронного средства платежа в присутствии работника кредитной, торговой или иной организации вводится пин-код, таким образом, модифицируется компьютерная информация: решения данной проблемы нет ни на законодательном уровне, ни в разъяснениях высшей судебной инстанции. На наш взгляд, квалификация должна осуществляться по ст. 159.3 УК РФ в силу того, что введение пин-кода карты является лишь составной частью способа совершения преступления.

Результатом рассматриваемого преступления является материальный ущерб в виде похищенных у организаций или у физических лиц денежных средств, которые, как правило, находятся на их счѐте, то есть, денежных средств, не выраженных физически. Само преступление также является корыстным, то есть, корыстный мотив здесь является обязательным условием

[1] Приговор Первомайского районного суда г. Владивостока от 02.06.2018 по уголовному делу № 2-2876/2018. // Архив Первомайского районного суда г. Владивостока. 2018. Д. 2876/2018. Л. Д. 225.

субъективной стороны, целью совершения преступления является также именно хищение денежных средств[1].

Действительно, в ходе совершения этого преступления ущерб может быть нанесен в том числе и кредитно-финансовым организациям, но в судебной практике нередки случаи причинения материального ущерба в результате совершения рассматриваемого преступления, как и другим видам организаций, так и физическим лицам.

Так, приговором Пушкинского районного суда г. Санкт-Петербурга от 04 апреля 2017 года по делу № 1–74/2017 подсудимый Логунов М.В. был осуждѐн за совершение преступлений, предусмотренных ч.3 ст.159.6 УК РФ, ч. 3 ст. 183 УК РФ. Суд установил, что Логунов М. В., будучи сотрудником салона связи «МегаФон», внес в базу данных ПАО «Мегафон» фиктивные сведения об оформлении номера телефона сотовой связи подключенного к лицевому счету абонента, после чего осуществил регистрацию и выпуск сим-карты с этим номером телефона, после чего передавал их соучастникам. Они же производили перечисление денежных средств с лицевого счета абонента на подконтрольные этим неустановленным лицам счета третьих лиц[2]. В данном случае совершенно очевидно, что основной ущерб в виде похищенных денежных средств причинен был именно обладателям ранее упомянутых лицевых счетов, то есть физическим лицам, а потому говорить о том, что основным объектом рассматриваемого состава преступления являются отношения в сфере экономической деятельности, не представляется верным.

По делу № 1-95/2019 преступник гр. «Л.Р.В.» совершил мошенничество в сфере компьютерной информации. Гр. «Л.Р.В.» преследовал следующую

---

[1] Адашевский, Г. Мошенничество в сфере компьютерной информации: проблемы законодательной регламентации / Г. Адашевский // Уголовная политика и правоприменительная практика : Сборник материалов IX Международной научно-практической конференции, Санкт-Петербург, 11 марта 2022 года / Под общей редакцией Е.Н. Рахмановой. – Санкт-Петербург: Центр научно-информационных технологий "Астерион", 2022. – С. 646-654.

[2] Приговор Пушкинского районного суда г. Санкт-Петербурга от 4 апреля 2017 г. по делу № 1–74/2017. – URL: https://sudact.ru/regular/doc/KfAZx4gNIDNV/ (дата обращения: 07.10.2023).

цель: нарушение характеристик защищаемых объектов путем модификации, разрушения или блокирования программных и технических средств, ознакомления с защищаемой информацией, а также навязывания ложной информации или побуждения к принятию неверных решений. Следует отметить, что преступник руководствовался корыстными мотивами[1].

Предметом данного вида мошенничества являются имущество или право на имущество.

Предметом преступления становится чужое имущество, хищение или приобретение права, на которое осуществляется путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей[2].

К сожалению, в настоящее время законодатель не рассматривает криптовалюту цифровым правом. Но следует отметить, что до момента включения в состав имущества в цифровые права, суды признают криптовалюту в качестве цифровых прав. В качестве примера, приведем дело № А40- 124668/2017, по рассмотрению которого Девятый арбитражный апелляционный суд отнес криптовалюту в качестве имущества. В обоснование суд отметил, что перечень гражданско-правовых интересов в гражданском законодательстве страны является публичным в силу диспозитивности норм.

Кроме того, суд указывал на то, что действующее гражданское законодательство не содержит определения термина «иное имущество», указанного в ст. 128 ГК РФ, и допускает его предельно расширительное

---

[1] Приговор Октябрьского районного суда г. Владимира № 1-95/2019 от 4 июня 2019 г. по делу № 1-95/2019. – URL: https://sudact.ru/regular/doc/v59eyhN7lzJq/ (дата обращения: 07.10.2023)

[2] Абдульмянова, Т. В. Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ): понятие, уголовно-правовая характеристика и некоторые особенности расследования / Т. В. Абдульмянова, И. П. Асанова, В. В. Данилов // Вопросы российского и международного права. – 2021. – Т. 11, № 1А. – С. 134-145. – DOI 10.34670/AR.2020.23.36.021.

толкование с учетом нынешних экономических реалии и уровень цифровизации. Суд также принял во внимание норму ст. 6 ГК РФ, сущность которой заключается в том, что при невозможности использования аналогии закона вступают в силу общие принципы и смысл гражданского права и требования справедливости сила, добросовестность и разумность, в соответствии с которыми определяются права и обязанности сторон[1].

Из вышеприведенного примера можно сделать вывод, что криптовалюту можно считать в качестве собственности (имущества) и может быть предметом криминального вмешательства.

Преступление признается оконченным с момента получения виновным суммы денег (чужого имущества), а равно приобретения им юридического права на распоряжение такими деньгами (имуществом).

Так, в Мотовилихинском районе Перми состоялся суд над местным жителем 1993 г. рождения. Он признан виновным в совершении одиннадцати преступлений, предусмотренных ч. 2 ст. 272 УК РФ (неправомерный доступ к компьютерной информации), пяти преступлениях, предусмотренных ч. 1 и ч. 2 ст. 159.6 УК РФ (мошенничество в сфере компьютерной информации), и двух покушениях на мошенничество в сфере компьютерной информации. Как установило следствие, в мае 2017 г., располагая неправомерным доступом к охраняемой законом компьютерной информации, он модифицировал данные пользователей популярного интернет-магазина, на личных счетах которых имелись денежные средства. Их можно было использовать на приобретение различных товаров. В результате информация о заказе приходила на его электронную почту, а не к истинному владельцу аккаунта. Таким образом, осужденный практически через день заказывал товары в интернет-магазине, что-то для себя, что-то на перепродажу. Некоторые покупки отменяли по причине отсутствия товара у поставщика, а денежные средства возвращали

[1] Постановление Девятого арбитражного апелляционного суда от 15 мая 2018 г. № 09АП16416/2018 по делу № А40-124668/2017. – URL: https://www.garant.ru (дата обращения: 20.10.2023).

пользователю, однако злоумышленника этот факт не останавливал. Он формировал новый заказ на приобретение вещей. Другие запросы на товар аннулировались сотрудниками сайта из-за подозрения в несанкционированном доступе. Некоторые пользователи сами выявляли взлом, когда не могли получить доступ к учетной записи. Граждане немедленно обращались в клиентский центр, а заказы интернет-преступника также аннулировались[1].

В процессе расследования правоохранительными органами было установлено, что гр. «Л.К.А.» осуществляя свои функции в фирме «…» получал для ремонта системные блоки от ЗАО «…». Также было установлено, что гр. «Л.К.А.» обладая специальными познаниями в системе программирования и имея определенные программные средства, скопировал необходимые данные при проверке внутреннего наполнения системных блоков для получения информации (пароли и учетные записи пользователей). После преступных действий гр. «Л.К.А.» вскрывал учетные записи сотрудников ЗАО «…» и скачивал видеоматериалы в ночное время[2].

До другому делу гр. «С.М.С.» находился по адресу «…» ДД.ММ.ГГ. вступил в преступную группу, которую создан гр. 1 (неизвестных следствию), которая занималась хищением денег посредством обмана в сфере продажи авиабилетов в целях обогащения. Вовлеченный в преступную группу гр. «С.М.С.» осуществлял поиск участников для открытия банковских карт в кредитных организациях и осуществления безналичных переводов. В процессе осуществления своих полномочий гр. «С.М.С.» вовлек гр. 3, на которого были возложены обязанности по открытию банковских карт и привязыванием в мобильному банку. Реализую свои полномочия гр. 3 обратился к гр. 4, которая оформила банковскую карту «…» посредством

---

[1] В Перми вынесен приговор виновному в серии преступлений в сфере телекоммуникаций и компьютерной информации. URL: https://59.xn--b1aew.xn--p1ai/news/item/15783318 (дата обращения: 07.10.2023).

[2] Приговор по ст. 159.6 УК РФ // Московский городской суд. – URL: https://mos-gorsud.ru/ (дата обращения: 20.10.2023).

Интернета и установила мобильный банк с абонентским номером «…» за обещанное вознаграждение. После чего последняя получила от курьера банковскую карту «…» и передала гр. 3, который в свою очередь передал гр. «С.М.С.».

ДД.ММ.ГГ. для покупки авиабилета в Интернете из «…» в «…», гр. 5, применяя сеть Интернет и ноутбук марки «…» зашел на сайт «…», в которой содержатся ложные данные в сфере приобретения авиабилетов, ввел персональные данные и данные банковской карты. После чего с банковской карты гр. 5 были списаны деньги в размере «…» рублей на банковскую карту гр. 4, после чего были списаны деньги в размере «…» рублей на банковскую карту гр. 6. Размер похищенных денежных средств для гр. 5 является значительным[1].

Предлагаем рассмотреть еще одно уголовное дело, возбужденое в Якутии в отношении сотрудницы якутского управления федеральной почтовой связи АО «Почта России», при помощи программного обеспечения незаконно выписавшей себе выплаты на сумму более 41 млн рублей.

В сообщении говорится, что дело возбуждено в отношении руководителя группы расчета заработной платы. Подозреваемой предъявлено обвинение в совершении преступления, предусмотренном ч. 4 ст. 159.6 УК России. Женщина находится под подпиской о невыезде.

В ФСБ уточнили, что она незаконно начисляла себе выплаты путем ввода информации в программное обеспечение. Украденные таким образом средства она потратила на собственные нужды[2].

Следует отметить, что мошенничество в сфере компьютерной информации распространены среди сотрудников «Почты России». Так, в

---

[1] Постановление Вахитовского районного суда г. Казани № 1-413/2020 от 29 июля 2020 г. по делу № 1-413/2020. – URL: https://sudact.ru/regular/doc/ftR7s3xLHjHQ/ (дата обращения: 25.12.2023)

[2] Сотрудницу «Почты России» в Якутии обвиняют в хищении 41 млн рублей. URL:https://yakutia-daily.ru/sotrudniczu-pochty-rossii-v-yakutii-obvinyayut-v-hishhenii-41-mln-rublej// (дата обращения: 25.12.2023)

Чамзинском районе Мордовии начальница отделения почтовой связи вместе с коллегой похитила у работодателя более 4 миллионов рублей. Две сотрудницы «Почты России» действовали по неклассической схеме. Идейным вдохновителем стала 31-летняя, окончившая девять классов школы, начальница отделения связи в чамзинском селе Отрадное – Оксана Перепелова. К криминальному бизнес-проекту она привлекла 33-летнюю коллегу Веру Булутову, которая осуществляла контроль за денежными переводами в отделении села Репьевка.

Перепелова была заведующей, она контролировала все транзакции. Женщина создавала операции по переводу денег на карту Булутовой и, когда они зачислялись, то отменяла операцию якобы из-за «ошибочного перевода». Затем заведующая брала карту Веры и обналичивала деньги, а потом удаляла информацию из служебного компьютера. За четыре месяца схема обогатила работниц учреждения на 4 миллиона 100 тысяч рублей. Раскрыть эту схему удалось оперативникам регионального УФСБ.

Следственным отделом Управления в отношении 31-летней женщины возбуждены и расследованы уголовные дела по ч. 3 ст. 160 УК РФ, ч. 4 ст. 159.6 УК РФ, ч. 4 ст. 274.1 УК РФ. В отношении 33-летней фигурантки возбуждено уголовное дело по ч. 5 ст. 33, ч. 4 ст. 159.6 УК РФ.

Деньги представительницы прекрасного пола пускали на развлечения, походы в массажные салоны и салоны красоты. Булутова вину признала частично, а Перепелова – все отрицает, ссылаясь на то, что надзорный орган в лице коллеги пропускал же операции, следовательно, ничего не законного она не сделала. Несмотря на непризнание вины, правоохранителям удалось собрать достаточное количество улик, подтверждающих вину обеих работниц. Материалы дела с утвержденным обвинительным заключением направили на рассмотрение в суд[1].

[1] В Мордовии две сотрудницы «Почты России» похитили более 4 миллионов рублей и пошли по салонам красоты. URL: https://www.info-rm.com/2022/08/19/v-mordovii-dve-

Завершая рассмотрение вопроса, поставленного в рамках настоящего параграфа, необходимо и целесообразно сформулировать следующие выводы:

Объективная сторона преступления, предусмотренного ст. 159.6 УК РФ, характеризуются следующими способами:

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

2) иное вмешательство в информационную сеть или информационно-телекоммуникационную сеть.

Обязательными объективными признаками для данных составов преступления выступают преступные последствия, под которыми понимается вред, причиненный потерпевшему (могут быть в значительном, крупном, особо крупном размере), и причинно-следственная связь между преступным деянием и ими.

§ 2. Субъективные признаки мошенничества в сфере компьютерной информации

В настоящем параграфе рассмотрим субъект и субъективную сторону мошенничества в сфере компьютерной информации.

В соответствии со ст. 19 УК РФ «Уголовной ответственности подлежит только вменяемое физическое лицо, достигшее возраста, установленного настоящим Кодексом»[1]. Данные признаки обязательны для квалификации общественно опасного деяния как преступления. Отсутствие хотя бы одного

sotrudnitsy-pochty-rossii-pokhitili-bolee-4-millionov-rubley-i-poshli-po-salonam-kras/ (дата обращения: 20.03.2024).

[1] Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ // Справ.-правовая система «КонсультантПлюс» (дата обращения: 25.12.2023).

из данных признаков исключает наличие субъекта преступного посягательства.

Субъект – вменяемое дееспособное лицо, достигшее 16-летнего возраста. Однако ч. 3 ст. 159.6 УК РФ предусматривает собой ответственность за совершение преступления специальным субъектом – лицом с использованием своего служебного положения – должностными лицами, обладающими признаками, предусмотренными п. 1 примечаний к ст. 285 УК РФ, государственных или муниципальных служащих, не являющихся должностными лицами, а также иных лиц, отвечающих требованиям, предусмотренным п. 1 примечаний к ст. 201 УК РФ (например, лицо, которое использует для совершения хищения чужого имущества свои служебные полномочия, включающие организационно-распорядительные или административно-хозяйственные обязанности в коммерческой организации)[1].

Так, Приговором Якутского городского суда Республики Саха (Якутия) от 30 июня 2022 года рассмотрено уголовное дело № 1-1082/2022 в отношении Г.Р.В. по обвинению в совершении преступлений, предусмотренных ч. 4 ст. 159.6, ч. 4 ст. 159.6 УК РФ. Судом установлено, что подсудимый Г.Р.В., осуществляя свою трудовую деятельность в банке в должности главного персонального менеджера, имея доступ к компьютерной автоматизированной банковской системе, находясь на своем рабочем месте в операционном офисе, совершал хищение денежных средств с банковских счетов клиентов банка, в том числе по первому эпизоду со счета С.П.Р., заменив действующий номер телефона клиента С.П.Р. на свой номер телефона тем самым, ввел и модифицировал компьютерную информацию и получил доступ к личному кабинету клиента без соответствующего обращения клиента, после чего, имея доступ к личному кабинету С.П.Р., оформил на него выдачу банковской карты, которую привязал к его банковскому счету и совершил хищение денежных средств С. П.Р., хранящихся на счетах Банка в общей сумме 1 022 573 рубля,

[1] О судебной практике по делам о мошенничестве, присвоении и растрате: Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 // Российская газета. – 2017. – № 280.

чем причинил последнему материальный ущерб в особо крупном размере. Также аналогичным образом Г.Р.В. путем ввода модификации компьютерной информации совершил хищение денежных средств К.Л.К., хранящихся на счетах Банка, в сумме 3 486 607 рублей 31 копейки, причинив потерпевшему ущерб на общую сумму, с учетом комиссии Банка, в размере 3 488 407 рублей 31 копейка, то есть в особо крупном размере.

Окончательное наказание подсудимому Г.Р.В. по совокупности совершенных им преступлений назначено судом по правилам ч.ч. 3, 4 ст. 69 УК РФ - путем частичного сложения наказаний в виде 6 лет лишения свободы условно с испытательным сроком три года, с ограничением свободы сроком на 01 год, без штрафа[1].

Так, в Якутии состоится рассмотрение уголовного дела о мошенничестве в сфере компьютерной информации. На скамье подсудимых окажется теперь уже бывшая работница банка, которая решила обогатиться за счёт клиента.

В ходе расследования было установлено, что женщина умышленно изменила данные умершего клиента банка, обладая доступом к базе кредитной организации. Она привязала к банковскому счёту клиента свой номер телефона, после чего воспользовалась чужими деньгами, потратив их на личные нужды. Сумма похищенных средств превысила 1,5 миллиона рублей.

Во время следственных действий женщина признала свою вину и заявила, что хотела вернуть деньги, но подвела память. Дело находится в суде[2].

Субъект расширяет традиционно понимаемый тайный способ совершения деяния, присущий краже, поскольку без ведома потерпевшего совершает вмешательство в компьютерную информацию, манипулируя

---

[1] Приговор №1-1082/2022 от 30 июня 2022 г. по делу №1-1082/2022. URL: https://jakutsky--jak.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=25069293&delo_id=1540006&new= 0&text_number=1 (дата обращения: 10.12.2023).

[2] Работница одного из отделений банков в Якутии присвоила деньги умершего клиента. URL: https://nerulife.ru/rabotnica-odnogo-iz-otdeleniy-bankov/ (дата обращения: 20.03.2024).

личной идентифицирующей информацией жертвы, чем нарушает установленный правопорядок в информационном пространстве, обеспечивающий его безопасное использование участниками информационных отношений, выступающий в качестве их дополнительного объекта[1].

Согласно действующему уголовному законодательству, вина может выступать в одной из двух форм: это в форме умысла или в форме неосторожности (ст.ст. 25 и 26 УК РФ). Субъективная сторона данного преступления предполагает прямой конкретизированный умысел и корыстную цель.

Субъективная сторона – прямой конкретизированный умысел. О наличии умысла, направленного на мошенничество в сфере кредитования, могут свидетельствовать, в частности, заведомое отсутствие у виновного лица права на вторжение в информационные базы потерпевших.

Перечисленные обстоятельства сами по себе не обязательно свидетельствуют о наличии мошенничества в сфере компьютерных информаций, в каждом конкретном случае должно быть достоверно установлено, что лицо, совершившее определенные в диспозиции комментируемой статьи действия, заведомо намеревалось использовать полученную информацию в корыстных целях.

Законом предусмотрены как квалифицированный состав — мошенничество в сфере компьютерной информации, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба потерпевшему (ч. 2), так и особо квалифицированные составы данного преступления: во-первых, деяния, совершенные с использованием виновными своего служебного положения, а равно в крупном размере (ч. 3); во-вторых,

[1] Власов, В. А. Отдельные актуальные правовые аспекты мошенничества с использованием компьютерной информации / В. А. Власов, В. А. Кондратова, И. В. Морозова // Аграрное и земельное право. – 2020. – № 11(191). – С. 159-162. – DOI 10.47643/1815-1329_2020_11_159.

деяния, совершенные организованной группой либо в особо крупном размере (ч. 4).

По материалам дела следует, что гр. Х. ДД.ММ.ГГ. отбывал наказание в ИК № «…» УФСИН России по «…». В процессе отбывания наказания у гр. Х. возник умысел на создание организованной группы и руководство ею для хищения денег с счетов граждан, которые обслуживаются в банке «…» в корыстных целях (для получения выгоды). Реализую свой умысел гр. Х. сформировал криминальную схему хищения денежных средств. Преступные действия гр. Х. предлагал осуществлять посредством GSM-каналов на сайте Авито. Ранее, гр. Х. приобрел sim-карты различных операторов страны, которые были зарегистрированы на «подставных» граждан.

Участники организованной группы осуществляли отправку сообщения или звонки посредством GSM-каналов с намерениями купить тот или иной товар. Участники организованной группы находя жертв, заявляли им о том, что могут оплатить посредством банковской карты «…». После чего просили жертв отправить им номер карты и копию паспорта владельца, которые без раздумья отправляли данные преступникам. После чего преступники, используя программу, позволяющую изменять номера, звонили в службу поддержки банка «…» и представились от именно других лиц с данными, которые были приобретены ранее, и просили идентификатор для входа в онлайн банка.

Работники банка «…» предоставляли идентификатор и отправляли 5-тизначный код. В последующем участники организованной группы повторно звонили жертвам и представлялись работников банка и просили продиктовать 5-тизначный код в целях оплаты. После получения кода и имеющегося идентификатора, преступники заходили в онлайн банк «…» и осуществляли перевод с карты жертв на другие счета, которые ранее были созданы для «отмывания»[1].

[1] Приговор Засвяженского районного суда г. Ульяновска по делу № 2-1/2018 // Ульяновский городской суд. – URL: http://zasvijajskiy.uln.sudrf.ru/ (дата обращения: 10.12.2023).

Субъективную сторону мошенничества в сфере компьютерной информации образует прямой умысел на завладение чужим имуществом посредством незаконного вторжения в функционирование средств компьютерной информации.

Так, прокуратура Тюменской области направила в Центральный районный суд Тюмени уголовное дело в отношении 31-летнего жителя Перми за хищение более 10,5 млн руб. Он обвиняется по ч. 4 ст. 159.6 УК РФ (мошенничество в сфере компьютерной информации, совершенное группой лиц по предварительном сговору, с банковского счета, в особо крупном размере), и ему грозит лишение свободы на срок до 10 лет. Следствие установило, что в мае 2020 г. обвиняемый совместно с неустановленным лицом реализовал план по хищению крупной денежной суммы у строительной фирмы в Ялуторовске (Тюменская область). Они отправили на электронную почту застройщика вредоносную компьютерную программу. С ее помощью мошенники получили удаленный доступ к расчетному счету организации и под видом зарплаты перевели на свои банковские карты более 10,5 млн руб. Согласно договоренности, мужчина вывел деньги в банкоматах Краснодара, из которых оставил себе 300 тыс. руб., а остальные средства были переведены в биткоины. В ходе розыска он был задержан краснодарской полицией и заключен под стражу по решению суда. Обвиняемый в ходе следствия вернул организации больше, чем похитил (11,9 млн руб.). Уголовное дело в отношении соучастника выделено в отдельное производство. Ранее суд в Омске назначил штраф разработчику вредоносных программ, получающих доступ к номерам банковских карт, адресам электронных почт и аккаунтам различных сервисов для получения незаконной выгоды[1].

Таким образом, следует отметить, что преимущественно субъектом преступления, предусмотренного ст. 159.6 УК РФ выступает общий субъект – физическое вменяемое лицо, достигшее возраста уголовной ответственности,

[1] В Тюмени будут судить жителя Перми за хищение 10,5 млн рублей с помощью вирусного ПО. URL: https://www.kommersant.ru/doc/4637386 (дата обращения: 07.10.2023).

но бывают и случаи, когда исследуемые преступления совершаются специальным субъектом (п. «а» ч. 3 ст. 159.6 УК РФ). Как правило к данным субъектам следует относить сотрудников банковских организаций.

Субъективная стороны преступления, предусмотренного ст. 159.6 УК РФ характеризуется прямым, конкретизированным умыслом, о котором свидетельствуют совершенные действия преступников.

ГЛАВА 2. УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА МОШЕННИЧЕСТВО В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

§ 1. Актуальные вопросы разграничения мошенничества в сфере компьютерной информации от иных смежных составов

Отдельного внимания заслуживает вопрос о конкуренции и (или) совокупности статьи 159.6 УК РФ с другими составами. Проблем разграничения статьи 159 УК РФ и статьи 159.6 УК РФ не возникает, так как доктриной уголовного права давно выработан подход, согласно которому при конкуренции общей и специальной нормы, квалификация должна осуществляться по специальной, то есть по статье 159.6 УК РФ, а в соответствии с частью 3 статьи 17 УК РФ совокупность преступлений в этом случае отсутствует. Отсутствует совокупность преступлений и в случаях, когда статья Особенной части УК РФ предусматривает другое преступление в качестве обстоятельства, влекущего более строгое наказание (ч. 1 ст. 17 УК РФ). Сравнивая санкции статьи 159.6 и статьи 272 УК РФ, можно увидеть, что данное правило может применяться в случаях совершения компьютерного мошенничества организованной группой, за которое наказание предусмотрено вплоть до 10 лет лишения свободы, тогда как наказание за неправомерный доступ к компьютерной информации, совершенный организованной группой, наказывается до 5 лет лишения свободы, а также при совершении компьютерного мошенничества, причинившего крупный ущерб, либо лицом с использованием своего служебного положения. В остальных случаях, очевидно, требуется дополнительная квалификация по ст. 272 УК РФ[1].

[1] Уголовное право России. Особенная часть : учебник для вузов / О. С. Капинус [и др.]. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 1189 с.

В литературе по этому вопросу имеют место достаточно категоричные формулировки. Так, специалисты пишут, что ст. 159.6 УК РФ является специальной по отношению к ст.ст. 272, 273 УК РФ. Суть ее рассуждений заключается в том, что неправомерный доступ к компьютерной информации из корыстной заинтересованности является действием, направленным на хищение, следовательно, компьютерная информация выступает средством доступа к чужому имуществу, что входит в объективную сторону ст. 159.6 УК РФ. В силу требований ч. 3 ст. 17 УК РФ дополнительной квалификации по ст.ст. 272, 273 УК РФ не требуется[1]. Следует учитывать то обстоятельство, что способы совершения компьютерного мошенничества лишь отчасти перекликаются с указанными в диспозиции ст. 272 УК РФ способами. Законодатель использует термин «иное вмешательство» в ст. 159.6 УК РФ, что позволяет утверждать, что способов совершения компьютерного мошенничества больше. Кроме того, при совершении мошенничества в сфере компьютерной информации доступ к этой информации может носить как законный, так и незаконный характер, тогда как в ст. 272 УК РФ речь идет о неправомерном доступе к охраняемой законом компьютерной информации. На наш взгляд, на данном обстоятельстве и следует строить ответ на вопрос о совокупности или отсутствии таковой составов преступлений, предусмотренных ст. 159.6 УК РФ и ст. 272 УК РФ, так как санкция ст. 159.6 УК РФ не позволяет дать однозначный ответ в соответствии с правилом, изложенным в ч. 1 ст. 17 УК РФ.

Учитывая, что состав преступления, предусмотренный статьей 159.6 УК РФ, относится к числу сложных преступлений, которые могут совершаться посредством других преступлений-способов, необходимо выработать общий подход к правилам квалификации в подобных случаях. Кроме того, авторы справедливо отмечают, что, если способ совершения преступления является

[1] Хисамова, З. И. Об особенностях квалификации преступлений, совершаемых в сфере использования информационно-коммуникационных технологий / З. И. Хисамова // Общество и право. – 2021. – № 1(55). – С. 117-120.

самостоятельным преступлением, его вменение по совокупности с основным преступлением не требуется. Такой вывод он сделал на основе правила о конкуренции общего и части[1], однако данное правило, хотя и взятое нами за основу, не во всех случаях применимо. В.В. Свечников, придерживаясь аналогичной позиции, добавляла, что преступление-способ не может вменяться только в том случае, если по тяжести он ниже основного состава преступления. В случае если тяжесть преступления-способа совпадает с основным преступлением, а тем более если выше, то требуется дополнительная квалификация[2]. Кроме того, по мнению В.Б. Боровикова, еще одним условием отсутствия совокупности преступлений должно быть единство объекта[3]. Относительно квалификации ст. 272 УК РФ с иными составами преступлений, где неправомерный доступ является преступлением-способом, В.И. Гладких указывал на необходимость определения вида совокупности: при реальной совокупности должна быть квалификация и по статье 272 и по основному составу, при идеальной совокупности оценка преступных действий дается только по основному составу[4], то есть в нашем случае только по статье 159.6 УК РФ.

Приведенные правила квалификации рассмотрим на конкретном примере. Так, Б.Н., Б.С., С.В. путем установки в Белгороде на банкоматы ПАО «Сбербанк России» устройства, предназначенного для негласного получения информации, намеревались совершить хищение денежных средств со счетов клиентов банков. Они предполагали считать электронную информацию с

---

[1] Уголовное право. Особенная часть. Краткий курс : учебное пособие для вузов / И. Я. Козаченко [и др.] ; ответственный редактор И. Я. Козаченко. – Москва : Издательство Юрайт, 2023. – 263 с.

[2] Сверчков, В. В. Уголовное право : учебник для среднего профессионального образования / В. В. Сверчков. – 10-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2023. – 727 с.

[3] Боровиков, В. Б. Уголовное право. Особенная часть : учебник для вузов / В. Б. Боровиков, А. А. Смердов ; под редакцией В. Б. Боровикова. – 7-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2023. – 505 с.

[4] Уголовное право. Особенная часть. Преступления в сфере экономики : учебник для вузов / В. И. Гладких [и др.] ; под общей редакцией В. И. Гладких, А. К. Есаяна. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2023. – 324 с.

карты памяти неизвестного устройства, крепившегося ими на банкоматы, и далее передать ее изготовителю поддельных карт, но в силу того, что они были задержаны сотрудниками полиции, довести свой преступный умысел до конца им не удалось. Все подсудимые были признаны виновными в совершении преступлений, предусмотренных ч. 2 ст. 35, ч. 3 ст. 183; ч. 3 ст. 30, ч 2 ст. 159.6 УК РФ[1].

При квалификации деяний правоприменитель должен исходить из того, на каких основаниях, то есть законных или незаконных, виновное в хищении лицо получило доступ к компьютерной информации. В случае законного доступа к такой информации дополнительной квалификации по ст.ст. 187, 272, 273 УК РФ не требуется. Итак, действующая редакция ст. 159.6 УК РФ нуждается в разъяснениях Пленума Верховного Суда РФ.

Полагаем, с учетом сложившейся правоприменительной практики и доктринального толкования форм хищения, судам следует дать разъяснения, что в случае, если хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей осуществляется с участием лица, воспринимающего искаженную информацию как истинную, например, «фишинг», смс-мошенничество, платный просмотр видеорекламы и т. п., содеянное следует квалифицировать как мошенничество в сфере компьютерной информации[2].

В случае осуществления хищения тем же способом, но без непосредственного участия человека, например, посредством использования автоматизированных систем, содеянное следует квалифицировать как кражу.

---

[1] Приговор Свердловского районного суда г. Белгорода. Дело № 1-64/2013. URL: https://sverdlovsky-blg.sudrf.ru (дата обращения: 07.10.2023).

[2] Алексеев, Д. С. Мошенничество в сфере компьютерной информации: особенности квалификации и конкуренции со смежными составами преступлений / Д. С. Алексеев // Аллея науки. – 2022. – Т. 1, № 2(65). – С. 508-518.

При решении вопроса о совокупности преступлений, например со статьями 183, 187, 272, 273 УК РФ, необходимо учитывать ряд условий:

1) определять основания доступа к компьютерной информации;

2) если доступ осуществлялся незаконно, правоприменитель должен дать юридическую оценку таких действий, основываясь на таких условиях квалификации как единство родового объекта и категория преступления.

Учитывая, что ч. 1 ст. 159.6 УК РФ относится с категории преступлений небольшой тяжести, данное обстоятельство свидетельствует о необходимости дополнительной квалификации по соответствующей статье УК РФ, являющейся по отношению к ст. 159.6 УК РФ преступлением-способом независимо от совпадения либо несовпадения родового объекта.

Для решения о наличии или отсутствии совокупности мы полагаем необходимым определить, является ли преступление, предусмотренное ст. 159.6 УК РФ многообъектным или нет, поскольку если мошенничество в сфере компьютерной информации имеет своим объектом только отношения собственности, то необходимость квалификации по совокупности существенно возрастает. Напротив, если мошенничество в сфере компьютерной информации охватывает причинение вреда как отношениям собственности, так и информационной безопасности, то в данной ситуации остро встаёт вопрос о нарушении принципа недопустимости двойного вменения при квалификации по совокупности.

Так, по мнению Е.Н. Бархатовой, мошенничество в сфере компьютерной информации имеет два предмета: компьютерную информацию и имущество[1]. Однако, в этой же статье Е.Н. Бархатова пишет о том, что «именно компьютерная информация, зачастую не являясь предметом посягательства, представляет собой обязательный элемент способа его совершения». Данное противоречие вызывает неоднозначность в позиции автора, однако,

[1] Бархатова, Е. Н. Мошенничество в сфере предпринимательства: теория, практика, проблемы / Е. Н. Бархатова, А. О. Миронов // Безопасность бизнеса. – 2021. – № 2. – С. 27-31. – DOI 10.18572/2072-3644-2021-2-27-31.

наталкивает на вывод о том, что всё-таки преступление, предусмотренное ст. 159.6 УК РФ нельзя считать многообъектным. При этом нельзя отрицать, что компьютерная информация (или информационная безопасность) тем не менее являются элементом состава данного преступления. Мы считаем, что компьютерная информация выполняет роль элемента не объекта, а объективная стороны, а именно средства совершения преступления. Такой же позиции придерживается Н.А. Лопашенко[1] в своих исследованиях.

Таким образом, с учетом того, что явного пересечения в объекте преступлений главы 28 УК РФ и мошенничества в сфере компьютерной информации не имеется, можно сделать вывод о допустимости двойной квалификации и проанализировать проблемы совокупности с каждым из составов.

Авторы, исследовавшие данный вопрос приходят к противоречивым выводам. Там, С.Я. Бойко указывает, что мошенничество в сфере компьютерной информации необходимо отличать от посягательств против компьютерной безопасности, однако, не предлагает критериев и не выдвигает варианты квалификаций[2].

Необходимо отметить, что при попытке предложить верный вариант квалификации, мы столкнулись с несколькими проблемами. Во-первых, основной проблемой является то, что в ст. 159.6 УК РФ и в преступлениях главы 28 УК РФ законодателем употребляются лишь частично пересекающиеся понятия. Трудно предположить, была ли в этом задумка законодателя, либо вышло ли это не нарочно.

Верховный Суд оставляет понятие «вмешательство» довольно открытым и неисчерпывающим, что в итоге делает перечень способов совершения деяние в ст. 159.6 УК РФ казуально-абстрактным.

---

[1] Лопашенко Н.А. Компьютерное мошенничество - новое слово в понимании хищения или ошибка законодателя? // Пермский юридический альманах. – 2019. – №2. – С. 598-608.

[2] Бойко С.Я. Уголовная ответственность за мошенничество: теоретико-прикладное исследование. М.: Юрлитинформ, 2019. – 198 с.

При этом в главе 28 УК РФ законодатель использует лишь четыре понятия: уничтожение, блокирование, модификацию и копирование. Соответственно, в ст. 159.6 УК РФ и главе 28 УК РФ есть полное совпадение по признакам «блокирование» и «модификация», смысловое совпадение по признаку «удаление» / «уничтожение» и различия по признакам «копирование» (который имеется в главе 28 УК РФ) и «ввод» (который имеется в ст. 159.6 УК РФ).

Тут необходимо отметить, что указанные выше признаки в сравниваемых составах выполняют разную роль. Так, в ст. 159.6 УК РФ указанные признаки выполняют роль альтернативных способов совершения деяния. При этом в ч. 1 ст. 272 УК РФ и ч. 1 ст. 274 УК РФ они выполняют роль опасных последствий, а в ч. 1 ст. 273 УК РФ и ч. 1 ст. 274.1 УК РФ – двойную роль преступной цели и альтернативного последствия, хотя некоторые авторы считают, что данный признак выполняет роль функционально-целевой характеристики преступного средства[1].

Во-вторых, необходимо сказать о сходстве терминов «уничтожение» и «удаление». Всё указывает на их тождество, однако, основным нюансом может быть потенциальная возможность восстановления утраченной информации, что и может быть критерием различия данных терминов. Однако, в соответствии с Методическими рекомендациями по осуществление прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации уничтожение информации – это приведение информации или ее части в непригодное для использования состояние независимо от возможности ее восстановления. Разъяснения термина «удаление», который используется в ст. 159.6 УК РФ, в нормативно-правовой базе не имеется. Однако, в связи с тем, что есть чёткое определения уничтожения, которое говорит о том, что возможность восстановления

[1] Савельев И.В. Мошенничество в сфере компьютерной информации: потенции квалификационных страданий / И.В. Савельев // Вопросы российской юстиции. – 2019. – №4. – С. 436-452.

информации не имеет значения, можно с уверенностью сказать, что термины «уничтожение» и «удаление» как минимум соотносятся как целое (в котором возможность восстановления не имеет значения) и частное (в котором возможность восстановления теоретически имеет значение). Соответственно, можно сделать вывод о взаимозаменямости и условном тождестве данных терминов.

В-третьих, что касается термина «ввод», который употребляется в ст. 159.6 УК РФ и не употребляется в главе 28 УК РФ, то необходимо отметить, что данный признак в принципе не является самостоятельным. Неправомерный ввод информации так или иначе повлечет её модификацию, а значит, что операция «ввод» является частью операции «модификация».

В-четвёртых, поскольку, как отмечалось выше, в ст. 159.6 УК РФ перечень способ совершения преступления является открытым, на самом деле исключает препятствия для рассмотрения последствия ст. 272 УК РФ «копирования» одновременно как способ совершения для 159.6 УК РФ в виде копирования, что также нивелирует терминологическую разницу при формулировке диспозиций составов. Некоторые авторы, однако, отмечают, что похищение путём копирования невозможно, однако, для нас данная позиция не является однозначной[1].

Соответственно, на первый взгляд кажется, что вышеизложенные признаки являются дублирующими, что указывает на их сходство и подвергает большому сомнению возможность квалификации по совокупности. Однако позиция Верховного Суда РФ однозначна – возможные причины этого мы разберем ниже. Тем не менее, в защиту позиции Верховного Суда РФ мы хотим отметить, что данные признаки в разных составах играют разную уголовно-правовую.

---

[1] Уголовная ответственность и наказание : учебное пособие для вузов / И. А. Подройкина [и др.] ; под редакцией И. А. Подройкиной. – 6-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2023. – 269 с.

Следует отметить, что ст. 159.6 УК РФ не анализирует вопрос правомерности доступа в принципе. Из этого следует, что в случае совершения мошенничества по ст. 159.6 УК РФ, когда доступ к информации был правомерным, возможность дополнительного вменения ст. 272 УК РФ исключается в принципе. Некоторые авторы полагают, что данный вывод противоречит Постановлению Пленума № 48, однако, мы с этим не согласны. В п. 20 Верховный Суд указывает, что квалификация по совокупности со ст.ст. 272, 273 и 274.1 УК РФ требуется только в случае мошенничества в сфере компьютерной информации, совершенного посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ.

§ 2. Назначение наказания за совершение мошенничества в сфере компьютерной информации

Одним из основных признаков преступления является его наказуемость. Наказание – основная мера уголовно-правового воздействия и основная форма реализации уголовной ответственности. С позиций уголовно-правовой теории и практики именно в существовании института наказания состоят смысл и суть уголовного права и уголовного законодательства. Для осуществления задач последнего уголовный закон устанавливает строго определенные виды наказаний, а их исчерпывающий перечень представляет систему уголовных наказаний.

Институту наказания в уголовно-правовой науке посвящено значительное число публикаций, которые регулярно пополняются новыми источниками, отражающими современные проблемы института наказания и

авторское понимание мер уголовно-правового воздействия и их назначения судом[1].

В исследуемой проблеме большинство уголовных дел связаны с совокупность при назначении наказания. «Соблюдая общие правила назначения наказания по совокупности преступлений, судам необходимо выполнять требования ч. ч. 2 и 3 ст. 69 УК РФ, согласно которым окончательное наказание по совокупности преступлений определяется путем полного или частичного сложения наказания и не может превышать более чем наполовину максимальный срок или размер наказания, предусмотренного за наиболее тяжкое из совершенных преступлений (ч. 2) или более чем наполовину максимальный срок наказания в виде лишения свободы, предусмотренный за наиболее тяжкое из совершенных преступлений (ч. 3)»[2].

«При назначении наказания по совокупности преступлений требуется определить как наказание за каждое из преступлений в отдельности, так и окончательное наказание за все совершенные преступные деяния»[3].

В соответствии с положениями ст. 159.6 УК РФ, предлагаем рассмотреть возможные виды наказаний по соответствующим частям и пунктам с примерами из правоприменительной практики.

Итак, за совершение преступлений, предусмотренных ч. 1 ст. 159.6 УК РФ, виновном могут назначаться следующие виды наказаний:

1) штраф в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года;

---

[1] Алферова, Е. В. Назначение уголовного наказания: системные исследования российских ученых-специалистов в области уголовного права, уголовного процесса, уголовно-исполнительного права и криминологии / Е. В. Алферова // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Серия 4: Государство и право. – 2020. – № 1. – С. 123-130.

[2] Умарова, А. А. Назначение наказания по совокупности преступлений / А. А. Умарова // Актуальные проблемы международных отношений в условиях формирования мультиполярного мира : сборник научных статей 11-й Международной научно-практической конференции, КУРСК, 13 декабря 2022 года. – курск: Юго-Западный государственный универси, 2022. – С. 308-311. – DOI 10.47581/2022/MO-25/Umarova.03.

[3] Чижова, В. П. Назначение наказания по совокупности преступлений / В. П. Чижова // Научная гипотеза. – 2018. – № 14. – С. 6-10.

2) обязательные работы на срок до трехсот шестидесяти часов;

3) исправительные работы на срок до одного года;

4) ограничение свободы на срок до двух лет;

5) принудительные работы на срок до двух лет;

6) арест на срок до четырех месяцев.

Приговором Димитровградского городского суда Ульяновской области от 22.08.2017 С.Ю.А. признали виновным в совершении преступлений, предусмотренных ч. 1 ст. 159.6 УК РФ и ч. 1 ст. 161 УК РФ. С.Ю.А. в целях незаконного завладения чужими денежными средствами, воспользовался похищенным планшетом, а именно сим-картой, которая в нем находилась и к которой была подключена услуга «Мобильный банк», совершил с ее помощью отправку смс-сообщений на номер «900» для перевода денежных средств на подконтрольный ему номер мобильного телефона. В результате со счета банковской карты потерпевшей произошло списание денежных средств.

Суд, вменяя состав преступления, предусмотренный ч. 1 ст. 159.6 УК РФ, учитывал, что отправка смс-сообщений на соответствующий номер, представляла собой ввод компьютерной информации в форме сигнала, что являлось способом совершения мошеннических действий и, следовательно, образовывало состав мошенничества в сфере компьютерной информации[1].

В соответствии с материалами уголовного дела № 1-146/2013 мирового суда судебного участка Ковдорского района Мурманской области в декабре 2013 г. подсудимый Р. был признан виновным в мошенничестве в сфере компьютерной информации по ч. 1 ст. 159.6 УК РФ. В приговоре была использована формулировка: «продолжая реализовывать свой преступный умысел, направленный на тайное хищение чужого имущества, Р. 13 июня 2013 года, находясь в г. Ковдоре, с абонентского номера направил смс-сообщение на единый абонентский номер ОАО «Сбербанк России», с указанием кодовой команды, осуществив вмешательство в функционирование банковского

[1] Приговор Димитровградского городского суда Ульяновской области от 22.08.2017. по делу №1-256/2017. URL: http://dimitrovgradskiy.uln.sudrf.ru/ (дата обращения: 29.12.2023).

сервера, на котором хранится информация о счетах клиентов ОАО «Сбербанк России». Суд избрал меру наказания в виде штрафа в размере «…» рублей[1].

По другому делу, возбужденному в отношении гр. Э., который совершил преступления, предусмотренные ч. 1 ст. 159.6 УК РФ и ч. 2 ст. 272 УК РФ, следует, что суд постановил о прекращении уголовного дела в соответствии со ст. 25 УПК РФ, поскольку гр. Э. примирился с потерпевшим[2].

Также следует отметить, что в правоприменительной практике имеются случаи, назначения судебного штрафа за совершение преступления, предусмотренного ч. 1 ст. 159.6 УК РФ. Так, гр. Н. посредством сети «…» совершил хищение денежных средств в сфере компьютерной информации, путем введения пароля и логина от сети «…» и отправления рассылки «друзьям» сообщений о просьбе в переводе денежных средств. Однако суд не желал привлекать гр. Н. к уголовной ответственности и назначать ему вид наказание.

Решая вопрос о размере судебного штрафа, суд руководствуется ст. 104.5 УК РФ и учитывает характер и степень тяжести совершенного им преступления, данные о личности подозреваемого, его имущественное положение и его семьи, возможность получения им дохода[3].

По другому делу, гр. С. был признан виновным в совершении преступления, предусмотренного ч. 3 ст. 30, ч. 1 ст. 159.6 УК РФ с назначением наказания в виде штрафа в размере 25 000 рублей. При этом, в процессе назначения наказания суд принимает во внимание характер и степень общественной опасности, сведения о личности подсудимого и прочее. Кроме того, смягчающими обстоятельствами выступают: явка с повинной, полное признание вины, деятельное раскаяние, состояние здоровья и оказание

---

[1] Приговоры судов по ст. 159.6 УК РФ Мошенничество в сфере компьютерной информации. Режим доступа: http://sud-praktika.ru/ (дата обращения: 29.12.2023).

[2] Постановление Сухиничского районного суда Калужской области по делу № 1-4-38/2021 от 16 апреля 2021 г. URL: https://clck.ru/37N3DL (дата обращения: 29.12.2023).

[3] Постановление Кудымкарского городского суда Пермского края по делу № 1-290/2018 от 20 декабря 2018 г. URL: https://clck.ru/37N3fy (дата обращения: 29.12.2023).

помощи бабушке и дедушке. Также, гр. С. положительно характеризуется по месту жительства, согласно рапорта УУП ОМВД «…» гр. ФИО1[1].

За совершение преступлений, предусмотренных ч. 2 ст. 159.6 УК РФ, виновном могут назначаться следующие виды наказаний:

1) штраф в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо

2) обязательные работы на срок до четырехсот восьмидесяти часов,

3) исправительные работы на срок до двух лет,

4) принудительные работы на срок до пяти лет с ограничением свободы на срок до одного года или без такового,

5) лишение свободы на срок до пяти лет с ограничением свободы на срок до одного года или без такового.

Итак, Зотов И.Л. совершил преступление, предусмотренное ч. 2 ст. 159.6 УК РФ в г. Кемерово, а после чего, действия Зотова И.Л. дополнительно квалифицировались по ч. 2 ст. 273 УК РФ. За совершение преступления, предусмотренное ч. 2 ст. 159.6 УК РФ суд своим приговором признал Зотова И.Л. виновным в совершении инкриминированного деяния с назначением наказания в виде лишения свободы до 2 лет. В соответствии со ст. 73 УК РФ назначенное наказание считать условным с испытательным сроком в 2 (два) года, обязав Зотова И.Л. встать в течение 1 месяца после вступления приговора в законную силу на учет в государственный специализированный орган ведающий исправлением осужденных, являться на регистрацию в указанный орган по установленному графику, не менять без уведомления уголовно – исполнительной инспекции постоянного места жительства, возместить заявленные исковые требования потерпевших в течении одного года с момента вступления приговора в законную силу[2].

---

[1] Приговор Мотовилихинского районного суда г. Перми по делу №1-72/2019 от 20 февраля 2019 г. URL: https://clck.ru/37N3Xj (дата обращения: 29.12.2023).

[2] Приговор Центрального районного суда г. Кемерово по делу № 1-573/2020 от 08 сентября 2020 г. URL: https://clck.ru/37N49E (дата обращения: 29.12.2023).

Так, в отношении гр. С. уголовное преследование по факту совершения преступления, предусмотренного ч. 2 ст. 159.6 УК РФ прекращено в соответствии со ст. 76.2 УК РФ, в связи с чем гр. С. был назначен судебный штраф в размере 10 000 рублей.

Согласно материал уголовного дела, гр. С. совершил мошенничество в сфере компьютерной информации, то есть хищение чужого имущества путем вмешательства в функционирование информационно телекоммуникационных сетей группой лиц по предварительному сговору, с причинением значительного ущерба гражданину, при следующих обстоятельствах.

Гр. С. ДД.ММ.ГГ. находился по адресу: «…», вступил в преступную группу, которая была сформирована неустановленными лицами, которые совершали хищение денежных средств посредством обмана путем продажи фиктивный авиабилетов. В целях реализации преступной деятельности, неустановленные лица, совместно с гр. С. создали в сети Интернет сайты, на которых находилась информация о приобретении авиабилетов. При этом, часть участников обеспечивали деятельность нескольких сайтов, которые в том числе предоставляли гражданам (пользователям) онлайн услуги по приобретению авиабилетов.

В свою очередь, гр. С. была отведена функция, связанная с приисканием соучастников для открытия банковских счетом в разных банковских организациях; легализацией денежных средств.

Таким образом, в действия гр. С. усматриваются признаки преступления, предусмотренного ч. 2 ст. 159.6 УК РФ. Однако, при расследовании преступления гр. С. заявил ходатайство о прекращении уголовного преследования с назначением ему меры уголовно-правового характера в виде судебного штрафа.

Суд при принятии решения руководствовался следующими обстоятельствами: полное возмещение вреда, совершение преступления впервые, отсутствие судимости (административных наказаний), преступление средней тяжести.

При определении размера судебного штрафа в соответствии со статьей 104.5 УК РФ и срока, в течение которого гр. С. обязан оплатить судебный штраф, суд принимал во внимание тяжесть совершенного противоправного деяния, материальное положение, и возможность получения заработной платы[1].

За совершение преступлений, предусмотренных п.п. «а», «б» или «в» ч. 3 ст. 159.6 УК РФ, виновном могут назначаться следующие виды наказаний:

1) штраф в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет;

2) принудительные работы на срок до пяти лет с ограничением свободы на срок до двух лет или без такового;

3) лишение свободы на срок до шести лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

До принятия Пленумом Верховного Суда РФ вышеуказанного постановления суды ошибочно квалифицировали содеянное по ст. 159.6 УК РФ. Примером может служить приговор по делу Г., осужденного по ч. 3 ст. 159.6 УК РФ. Имея умысел на хищение чужого имущества, Г., находясь в помещении торговой точки ЗАО «СЛ», будучи одетым в форму сотрудника данной организации и представившись новым сотрудником, введя, таким образом, в заблуждение находящегося на рабочем месте менеджера Н., путем обмана получил неправомерный доступ к персональному компьютеру и путем ввода компьютерной информации в программу «Парус 1С Продавец», осуществил три перевода денежных средств на счет принадлежащей ему

[1] Постановление Вахитовского районного суда г. Казани Республики Татарстан № 1-413/2020 от 29 июля 2020 г. по делу № 1-413/2020. URL: https://sudact.ru/regular/doc/ftR7s3xLHjHQ/ (дата обращения: 29.12.2023).

банковской карты, получив реальную возможность распоря.диться похищенными денежными средствам[1].

По другому делу гр. М. совершила противоправные действия, предусмотренные ч. 3 ст. 159.6 УК РФ при следующих обстоятельствах.

В период времени с ДД.ММ.ГГ. по ДД.ММ.ГГ. гр. М. осуществляла свои полномочия в должности специалиста по сопровождению корпоративных клиентов Поволжского филиала – «…» отделения ПАО «МегаФон», осуществлял обязанности по осуществлению мероприятий, связанных с сопровождением корпоративных клиентов, совершенствованием и сопровождением клиентов бизнес-сегмента и прочее. Также гр. М. предоставлен индивидуальный логин и пароль в целях осуществления своей служебной деятельности при использовании персонального компьютера и программных обеспечений ПАО «МегаФон», которые содержат в себе сведения о клиентах Поволжского филиала – «…» отделения ПАО «МегаФон», а также персональные данные их банковских и расчетных счетов.

В период времени с «…» ДД.ММ.ГГ. по «…» ДД.ММ.ГГ. у гр. М. возник преступный умысел, в связи с чем, находясь в офисе Поволжского филиала – «…» отделения ПАО «МегаФон», расположенный по адресу: «…», на совершение хищения чужого имущества в сфере компьютерной информации, а именно посредством ввода, модификации компьютерной информации, с применением своего служебного положения.

Так, гр. М. находясь в своем кабинете посредством ввода, модификации компьютерной информации, используя свое служебное положение, подключила к расчетному счету № «…», который зарегистрированный на МУ МВД России «…», абонентский номер. В дальнейшем гр. М. убедилась о том, что на расчетном счете имеются денежные средства в размере «…» с использованием информационно-биллинговой системы трансформировала

[1] Уголовное дело № 1-79/2013. Приговор Симоновского районного суда г. Москвы от 14 февраля 2013 г. // Справ.-правовая система «КонсультантПлюс» (дата обращения: 29.12.2023)

категорию клиента с «кредитный» на «предоплатный», статус клиента на «действующий», класс клиента на «корпоративный». В последующем, гр. М. перерегистрировала абонентский номер «…» на свой банковский счет для сокрытия следов противоправной деятельности. Для хищения денежных средств, гр. М. осуществляла переводы денежных средств на банковский счет, открытый на имя «…», который находился в пользовании гр. М., тем самым получив реальную возможность распоряжаться похищенными денежными средствами.

Материальный ущерб оценивается на общую сумму 28 853 руб. 24 коп.

С предъявленным обвинением гр. М. полностью согласилась, вину признала, заявила ходатайство о постановлении приговора без проведения судебного разбирательства.

При назначении наказания суд руководствуется принципом справедливости, а также учитывает характер и степень общественной опасности преступления, личность виновной, обстоятельства, смягчающие наказание, влияние назначенного наказания на исправление осужденной и на условия жизни ее семьи, все обстоятельства дела в их совокупности, конкретные обстоятельства дела.

В качестве смягчающих обстоятельств были признаны признание вины, деятельное раскаяние, активное способствование органам предварительного расследования, возмещение ущерба, состояние здоровья гр. М. Также при назначении наказания суд принимает во внимание характеристику с места работы и места жительства.

Таким образом, гр. М. признана виновной в совершении инкриминируемого деяния с назначением наказания в виде лишения свободы сроком на 2 года. В соответствии со ст. 73 УК РФ назначенное наказание считать условным с испытательным сроком 2 года[1].

---

[1] Приговор Фрунзенского районного суда г. Саратова № 1-66/2018 от 19 июля 2018 г. по делу № 1-66/2018. URL: https://sudact.ru/regular/doc/qtCZQWKOpk5x/ (дата обращения: 29.12.2023).

По другому делу, действия гр. М. квалифицировались как покушение на совершение преступления, предусмотренного п. «б» ч. 3 с. 159.6 УК РФ. Гр. М. работал в должности специалиста офиса продаж ПАО «…». Таким образом, гр. М. находился в офисе ПАО «…», расположенном по адресу: «…» в период времени с «…» по «…» ДД.ММ.ГГ., в связи с чем у него возник умысел на хищение чужого имущества в сфере компьютерной информации посредством переоформления абонентских номеров и сбыта от имени ПАО «…».

Реализуя свой преступный умысел, гр. М. нашел в сети Интернет сайт объявлений и позвонил по абонентскому номеру, указанному в объявлении и предложил приобрести «серебренные» и «золотые» абонентские номера. Потенциальный покупатель в свою очередь согласился на такое предложение гр. М. и заявил, что SIM-карты с абонентскими номера необходимо зарегистрировать на супругу – гр. Ш. В дальнейшем, гр. М., используя доступ к базам данных: «…», вошел в свою учетную запись и в учетную запись другого сотрудника – гр. Ю.. открыл официальный сайт ПАО «…», нашел подходящие абонентские номера и выписал их, после чего открыл программу «…» и запрограммировал пустой чип SIM-карты на индивидуальные абонентские номера.

Дальнейшие действия гр. М. заключались в следующем: он менял сведения владельца SIM-карты, печатал и подписывал заявления от имени гр. Ш. на смену владельца, отправлял на главный сервер ПАО «…» письма о смене владельца SIM-карты в целях активации абонентского номера и прочее. Таким образом, гр. М. посредством ввода и модификации компьютерной информации для хищения чужого имущества под учетными записями противоправно переоформлял «золотые» и «серебряные» абонентские номера на общую сумму «…». Однако действия гр. М. не было совершены до конца, поскольку сотрудниками ПАО «…» SIM-карты были заблокированы в связи с сомнительными операциями.

К смягчающим обстоятельствам суд относит: явку с повинной, активное способствование органам предварительного расследования, полное признание вины, наличие иждивенцев.

Таким образом, суд назначил гр. М. наказание в виде 1 года 6 месяцев лишения свободы, без штрафа, без ограничения свободы. На основании ст. 73 УК РФ назначенное наказание считать условным, с испытательным сроком 1 год[1].

За совершение преступлений, предусмотренных ч. 4 ст. 159.6 УК РФ, виновном могут назначаться следующие виды наказаний: лишение свободы на срок до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

Данные составы преступлений весь редки, однако встречаются в правоприменительной практике. Так, в 2019 г. по ч. 3 ст. 272, ч. 2 ст. 273 и ч. 4 ст. 159.6 УК РФ осуждены гр. Л. и гр. Б., которые в составе организованной группы получили неправомерный доступ к банкоматам одного из банков и возможность устанавливать на жесткие диски банкоматов файлы. После осуществления удаленного управление банкоматом участники организованной группы отправляли команды на выдачу денежных купюр в любом доступном объеме. В результате преступной деятельности с банкоматов было снято несколько миллионов рублей. Основная часть соучастников, в том числе организатор, не были установлены правоохранительными органами.

Таким образом, гр. Л. и гр. Б. по ч. 4 ст. 159.6 УК РФ были избраны виды наказания в виде 5 и 4 лет лишения свободы со штрафом 800 000 и 500 000 рублей, соответственно. В соответствии с ч. ст. 69 УК РФ путем частичного

---

[1] Приговор Советского районного суда г. Владивостока (Приморский край) № 1-277/2020 от 30 июля 2020 г. по делу № 1-277/2020. URL: https://sudact.ru/regular/doc/4AyuDmz7J9oX/ (дата обращения: 29.12.2023).

сложения наказаний по совокупности преступлений назначить окончательное наказание в виде 8 лет лишения свободы со штрафом 800 000 рублей – для гр. Л.; 7 лет лишения свободы со штрафом 500 000 рублей – для гр. Б. На основании ст. 73 УК РФ основное наказание назначенное подсудимым гр. Л. и гр. Б. считать условным с испытательным сроком 5 и 4 года соответственно.

При избрании меры наказания суд принимает во внимание в качестве обстоятельств, смягчающих наказание следующее: наличие малолетних детей, состояние здоровье, признание вины (частично), деятельное раскаяние, беременность супруги гр. Б., отсутствие судимостей, частичное возмещения вреда[1].

В правоприменительной практике имеются случаи, когда суды признают подсудимых виновными в совершении преступлений, предусмотренных ч. 1 ст. 159.6, ч. 1 ст. 159.6, ч. 1 ст. 159.6, ч. 4 ст. 159.6 УК РФ. Так, гр. И. совершил три преступления, предусмотренных ч. 1 ст. 159.6 УК РФ и одно преступление, предусмотренное ч. 4 ст. 159.6 УК РФ при следующих обстоятельствах. Гр. И. совершил преступление, являясь сотрудников ПАО «…», а именно: экономистом, с правом доступа к компьютерной информации и индивидуальному пароль для программного обеспечения «…» в целях работы с платежными картами.

Гр. И. ДД.ММ.ГГ. находился по адресу: «…», в период времени с «…» по «…», в связи с чем у него возник умысел на совершение вышеуказанного преступления, в связи с чем, он, используя доступ к компьютерной информации и индивидуальному пароль для программного обеспечения «…» ввел в базу данных недостоверные сведения, тем самым увеличив лимит денежных средств на банковском счета № «…», который принадлежит ему же. В последующем, гр. И. совершил еще два аналогичных преступлений, аналогичным способом и методом, с использованием одинаковых программ.

---

[1] Приговор Якутского городского суда (Республика Саха (Якутия)) № 1-681/2019 от 26 августа 2019 г. по делу № 1-1462/2018. URL: https://sudact.ru/regular/doc/8jIATe7oVfNK/ (дата обращения: 29.12.2023).

Кроме того, гр. И. находясь по адресу: «…», вступив в преступный сговор с гр. ФИО2 и иными неустановленными лицами, имея умысел на неправомерное завладение чужим имуществом – денежными средствами ПАО «…» в особо крупном размере, совершил противоправные действия, которые инкриминированы по ч. 4 ст. 159.6 УК РФ, при следующих обстоятельствах: гр. И. ДД.ММ.ГГ. находился по адресу: «…», в период времени с «…» по «…»используя доступ к компьютерной информации и индивидуальному пароль для программного обеспечения «…» ввел в базу данных недостоверные сведения, тем самым увеличив лимит денежных средств на банковском счета № «…», который открыт на гр. ФИО2, на общую сумму 25 953 015,15 руб. После чего, гр. ФИО2 совместно с гр. И. и иными неустановленными лицами, они распорядились похищенными денежными средствами по своему усмотрению.

При назначении наказания, суд принимает во внимание тот факт, что гр. И. на учете в ГНД и ГПНД не состоит, хронических психический расстройств не имеет, слабоумием не страдает. Кроме того, суд принимает во внимание характер и степень общественной опасности, личность гр. И. и смягчающие обстоятельства, к которым отнесены: отсутствие судимости (административным правонарушений), удовлетворительная характеристика с места жительства, положительная характеристика с места учебы и работы, полное признание вины, деятельное раскаяние, состояние здоровья, наличие грамот и благодарностей.

Таким образом, суд приговорил гр. И. к наказанию в виде обязательных работ на 240, 280 и 260 часов по первым эпизодам противоправной деятельности по ч. 1 ст. 159.6 УК РФ; в виде лишения свободы на срок 5 лет со штрафом в размере 250 000 рублей за преступление, предусмотренное ч. 4 ст. 159.6 УК РФ. Путем частичного сложения наказаний суд назначил гр. И. наказание в виде 5 лет 3 месяцев лишения свободы со штрафом в размере 250 000 рублей с отбыванием наказания в виде лишения свободы в исправительной колонии общего режима. Кроме того, суд приговорил гр. И. о

взыскании с него денежных средств в размере «…» и «…» в пользу ПАО «..2» в качестве материального ущерба[1].

Кировский районный суд рассмотрел уголовное дело 23-летнего омича и 24-летнего тюменца. Они обвинялись в мошенничестве в сфере компьютерной информации, совершенном группой лиц по предварительному сговору. Кроме того, жителю Тюмени было предъявлено еще одно обвинение в неправомерном воздействии на критическую информационную инфраструктуру РФ.

В конце 2022 года старший из осужденных получил доступ к базе данных клиентов. Это получилось за счет его обучения у работника, который занимался обслуживанием и продажами в компании сотового оператора.

Используя абонентские номера, предоставленные в мессенджере неустановленным лицом, вступившим с ним в сговор, скорректировал счета абонентов и вывел денежные средства на криптовалютные кошельки, а затем на банковские счета, похитив тем самым у компании 459 000 рублей. При следующей попытке хищения его профиль в компании оказался заблокирован.

Однако молодой человек решил не останавливаться на достигнутом. Вместе с другом из Омска и еще одним неустановленным мужчиной, с которым познакомился в даркнете, он придумал новую схему мошенничества.

Под видом начальника компании парень написал бывшей коллеге и потребовал логин и пароль от входа в систему. После аналогичным образом товарищи похитили 696 тыс. рублей. Еще одну попытку вывести средства уже пресекли сотрудники безопасности компании и ФСБ.

Виновные получили условные сроки. Омич – 1 год, а житель Тюмени – 3,5 года, также с последнего взыскали 714 тыс. рублей. Кроме того, оба парня должны заплатить сотовому оператору 128 тыс. рублей[2].

---

[1] Приговор Засвияжского районного суда г. Ульяновска по делу №1-376/2019 от 05 сентября 2019 года. URL: https://clck.ru/37N2ga (дата обращения: 29.12.2023).

[2] Омича осудили за хищение денег у абонентов сотового оператора. URL: https://omskinform.ru/news/188574 (дата обращения: 20.03.2024).

По другому делу, судом установлено, что подсудимый совместно с лицом (который за данные преступления уже осужден и отбывает наказание в местах лишения свободы) совершали хищение денежных средств путем ввода компьютерной информации. Роли между ними распределены были следующим образом: подсудимый отвечал за сбор и незаконное получение данных о чужих банковских картах, с помощью реквизитов которых осуществлял заказ и оплату товаров в интернет-магазинах. Затем он передавал информацию о заказе и месте его получения своему соучастнику, который в свою очередь получал заказ, оплаченный чужими банковскими картами, реализуя его и отправляя подсудимому либо выручку, либо же в случае невозможности его реализовать – сам товар.

Всего ими совершено семь преступлений на сумму 205 235 рублей. Подсудимый вину в совершенном преступлении признал. Осужденному назначено наказание в виде лишения свободы в колонии поселении сроком на 1 год и 8 месяцев[1].

Кировский районный суд г. Омска вынес приговор по уголовному делу в отношении двух граждан. Один из них признан виновным по п. «б» ч. 3 ст. 159.6 УК РФ, чч. 3-4 ст. 274.1 УК РФ, второй – по ч. 2 ст. 159.6 УК РФ.

Уголовное дело расследовалось СУ УМВД России по г. Омску на основании материалов, представленных УФСБ России по Омской области.

В суде установлено, что в октябре 2022 г. 24-летний осужденный, являясь учеником специалиста обслуживания и продаж в компании сотовой связи, получил доступ к базе данных клиентов. Осуществив корректировки сведений о балансе абонентских номеров, он вывел полученную сумму на криптовалютные кошельки, затем на сервисы электронных средств платежа и банковские карты, завладев почти 460 тыс. рублей, принадлежащих компании.

Кроме того, после прекращения ученического договора он ввел в заблуждение свою бывшую коллегу, получив обманным путем данные для

[1] Жителя Москвы осудили в Магадане за мошенничество в сфере компьютерной информации. URL: https://magadanmedia.ru/news/651923/ (дата обращения: 20.03.2024).

входа в систему. После чего по отработанной схеме совместно со вторым осужденным и еще одним лицом, уголовное дело в отношении которого выделено в отдельное производство, вывел еще около 700 тыс. рублей.

Очередную попытку хищения пресекли работники службы безопасности организации и сотрудники УФСБ. Вину в совершении преступлений мужчины признали, частично возместили причиненный ущерб.

Суд с учетом позиции государственного обвинителя назначил одному из них наказание в виде 3 лет 6 месяцев лишения свободы, второму – 1 года лишения свободы условно с испытательным сроком в 3 года и 1 год соответственно. С учетом частичного возмещения причиненного ущерба суд постановил взыскать с первого осужденного 714 тыс. рублей, а также с обоих солидарно почти 128 тыс. рублей в пользу компании сотовой связи[1].

Ковровским городским судом вынесен приговор в отношении двоих жителей Москвы и Новосибирска. Они признаны виновными в совершении 4 преступлений, предусмотренных ч. 2 ст. 273 УК РФ, 6 преступлений, предусмотренных ч. 3 ст. 272 УК РФ и 6 преступлений, предусмотренных ч. 4 ст. 159.6 УК РФ.

Обвинительное заключение утверждалось первым заместителем Генерального прокурора РФ А.В. Разинкиным.

Установлено, что мужчины, входя в состав организованной преступной группы, совместно с другими её участниками не позднее марта 2018 года создали и использовали вредоносные компьютерные программы, позволявшие удаленно управлять персональными компьютерами пользователей.

Обладая специальными познаниями в области компьютерной техники и программирования, осужденные создали общедоступные сайты, оформление и название которых соответствовали легальным сайтам бухгалтерской направленности, разместив на них замаскированные под электронные

[1] В Омске вынесен приговор двум местным жителям за мошенничество в сфере компьютерной информации. URL: https://epp.genproc.gov.ru/ru/web/proc_55/mass-media/news?item=93618539 (дата обращения: 06.03.2024).

бухгалтерские бланки и документы модули загрузки и управления вредоносными компьютерными программами.

Заражая компьютеры неопределённого круга лиц через сеть Интернет указанными программами, они получали возможность скрытного управления данными, после чего совершали дистанционные хищения.

Таким образом осужденные похитили денежные средства с расчетных счетов различных организаций из Ростовской, Свердловской, Вологодской и Владимирской областей на общую сумму свыше 16 млн рублей.

Приговором суда виновным назначено наказание в виде лишения свободы на срок 6 лет и 6 лет 6 месяцев соответственно с отбыванием в колонии общего режима[1].

Таким образом, следует вывод, что вид наказания за совершение преступлений, предусмотренных ч. 1, ч. 2, ч. 3, ч. 4 ст. 159.6 УК РФ может быть различным. Вид наказания избирается судом с учетом определенных сведений: степени и опасности преступного посягательства, наличие смягчающих и отягчающих обстоятельств, наличие судимости, характеристика по месту работы, жительства и учебы и много другое.

[1] Вынесен приговор по уголовному делу о создании и использовании вредоносных программ и мошенничестве в сфере компьютерной информации в особо крупном размере. URL: https://nashregion33.ru/news/vynesen-prigovor-po-ugolovnomu-delu-o-sozdanii-i-ispolzovanii-vredonosnyh-programm-i-moshennichestve-v-sfere-kompjuternoj-informacii-v-osobo-krupnom-razmere/ (дата обращения: 25.03.2024).

ЗАКЛЮЧЕНИЕ

Квалификация мошенничества по вышеназванным статьям УК РФ зависит, в первую очередь, от той сферы общественных отношений, в которой совершается данной преступление, а также от предмета преступного посягательства и способа совершения преступного деяния (критерии выделения специальных составов мошенничества).

В науке уголовного права деяние, предусмотренное ст. 159 УК РФ принято называть «простым» мошенничеством. Объективные и субъективные признаки данного вида мошенничества будут рассмотрены в следующей главе. В рамках данного параграфа необходимо определить сущность специальных видов мошенничества, а также степень их распространенности в общей структуре преступности.

На основании проведенного исследования объективных и субъективных признаков составления преступления, предусмотренные ст. 159.6 УК РФ, следует сделать следующие выводы. В уголовном праве к объективным признакам любого преступного деяния относятся его объект и объективная сторона.

Традиционно, под «объектом преступления» понимают общественные отношения, взятые под охрану уголовным законодательством.

Родовой объект мошенничества, как и других преступных деяний, как правило, совпадает с наименованием раздела Уголовного закона, в который включена соответствующая статья – Раздел VIII. Преступления в сфере экономики.

Видовой объект определяется главой Уголовного закона, в которой содержится конкретная статья, в данном случае ст. 159.6 УК РФ – глава 21. Преступления против собственности.

К предмету преступного посягательства могут относится различные элементы:

1) компьютерная информация;

2) имущество;

3) Интернет-трафик и многое другое.

В процессе цифровизации на современном этапе развития общества, большое внимание отводится новой «валюте» – криптовалюте. Согласно изученным материалам правоприменительной практики мы можем сделать вывод, что криптовалюту можно считать в качестве собственности (имущества) и она может быть предметом криминального вмешательства.

Кроме того, суды указывают на то, что действующее гражданское законодательство не содержит определения термина «иное имущество», указанного в ст. 128 ГК РФ, и допускают его предельно расширительное толкование с учетом нынешних экономических реалии и уровень цифровизации.

Суды также принимают во внимание норму ст. 6 ГК РФ, сущность которой заключается в том, что при невозможности использования аналогии закона вступают в силу общие принципы и смысл гражданского права и требования справедливости сила, добросовестность и разумность, в соответствии с которыми определяются права и обязанности сторон.

При рассмотрение объективной стороны особое внимание хотелось бы обратить внимание на способ совершения преступления.

Согласно материалам правоприменительной практики по уголовным делам, предусмотренных ст. 159.6 УК РФ, выделяются несколько способов преступных действий:

1) взлом с последующим хищением данных;

2) оформление банковских карт с применением краденных данных жертвы;

3) кремминг;

4) «инвестиционные копилки»;

5) покупка акций по минимальной цене и распространение заведомо ложные сведения о юридическом лице через информационное пространство

для создания большого спроса на них, ссылаясь на обладание секретной информацией о важном корпоративном событии;

6) использование электронных платежных средств (WebMoney, Яндекс.Деньги, Assist, Robox, Qiwi и др.);

7) спуффинг-атаки;

8) псевдоблаготворительность.

Объективная сторона мошенничества в сфере компьютерной информации отличается собственной уникальностью. Законодатель, сохранив мошеннические формы (хищение и приобретение права на чужое имущество), исключил традиционные способы совершения деяния (обман, злоупотребление доверием). Вместо них объективная сторона характеризуются следующими способами:

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

2) иное вмешательство в информационную сеть или информационно-телекоммуникационную сеть.

Разъяснения термина «удаление», который используется в ст. 159.6 УК РФ, в нормативноправовой базе не имеется. Однако, в связи с тем, что есть чёткое определения уничтожения, которое говорит о том, что возможность восстановления информации не имеет значения, можно с уверенностью сказать, что термины «уничтожение» и «удаление» как минимум соотносятся как целое (в котором возможность восстановления не имеет значения) и частное (в котором возможность восстановления теоретически имеет значение). Соответственно, можно сделать вывод о взаимозаменямости и условном тождестве данных терминов.

Что касается термина «ввод», который употребляется в ст. 159.6 УК РФ и не употребляется в главе 28 УК РФ, то необходимо отметить, что данный признак в принципе не является самостоятельным. Неправомерный ввод информации так или иначе повлечет её модификацию, а значит, что операция «ввод» является частью операции «модификация».

Субъект – вменяемое дееспособное лицо, достигшее 16-летнего возраста. Однако ч. 3 ст. 159.6 УК РФ предусматривает собой ответственность за совершение преступления специальным субъектом – лицом с использованием своего служебного положения.

Следует отметить, что у множества уголовным дел субъектом преступления, предусмотренного ст. 159.6 УК РФ – это сотрудники банковских и кредиторских организаций, которые имеют доступ к базам (системам) данных и индивидуальным паролям (ключам).

Согласно действующему уголовному законодательству и мнениям авторов, вина может выступать в одной из двух форм: это в форме умысла или в форме неосторожности (ст.ст. 25 и 26 УК РФ). На наш взгляд, субъективная сторона данного преступления предполагает прямой конкретизированный умысел и корыстную цель.

Субъективную сторону мошенничества в сфере компьютерной информации образует прямой умысел на завладение чужим имуществом посредством незаконного вторжения в функционирование средств компьютерной информации.

Для решения о наличии или отсутствии совокупности мы полагаем необходимым определить, является ли преступление, предусмотренное ст. 159.6 УК РФ многообъектным или нет, поскольку если мошенничество в сфере компьютерной информации имеет своим объектом только отношения собственности, то необходимость квалификации по совокупности существенно возрастает. Напротив, если мошенничество в сфере компьютерной информации охватывает причинение вреда как отношениям собственности, так и информационной безопасности, то в данной ситуации остро встаёт вопрос о нарушении принципа недопустимости двойного вменения при квалификации по совокупности.

Мошенничество в сфере компьютерной информации имеет два предмета: компьютерную информацию и имущество. «Именно компьютерная информация, зачастую не являясь предметом посягательства, представляет

собой обязательный элемент способа его совершения». Данное противоречие вызывает неоднозначность в позиции автора, однако, наталкивает на вывод о том, что все-таки преступление, предусмотренное ст. 159.6 УК РФ нельзя считать многообъектным. При этом нельзя отрицать, что компьютерная информация (или информационная безопасность) тем не менее являются элементом состава данного преступления. Мы считаем, что компьютерная информация выполняет роль элемента не объекта, а объективная стороны, а именно средства совершения преступления.

Необходимо отметить, что при попытке предложить верный вариант квалификации, мы столкнулись с несколькими проблемами. Во-первых, основной проблемой является то, что в ст. 159.6 УК РФ и в преступлениях главы 28 УК РФ законодателем употребляются лишь частично пересекающиеся понятия. Трудно предположить, была ли в этом задумка законодателя, либо вышло ли это не нарочно. Верховный Суд оставляет понятие «вмешательство» довольно открытым и неисчерпывающим, что в итоге делает перечень способов совершения деяние в ст. 159.6 УК РФ казуально-абстрактным.

При этом в главе 28 УК РФ законодатель использует лишь четыре понятия: уничтожение, блокирование, модификацию и копирование. Соответственно, в ст. 159.6 УК РФ и главе 28 УК РФ есть полное совпадение по признакам «блокирование» и «модификация», смысловое совпадение по признаку «удаление» / «уничтожение» и различия по признакам «копирование» (который имеется в главе 28 УК РФ) и «ввод» (который имеется в ст. 159.6 УК РФ).

Тут необходимо отметить, что указанные выше признаки в сравниваемых составах выполняют разную роль. Так, в ст. 159.6 УК РФ указанные признаки выполняют роль альтернативных способов совершения деяния. При этом в ч. 1 ст. 272 УК РФ и ч. 1 ст. 274 УК РФ они выполняют роль опасных последствий, а в ч. 1 ст. 273 УК РФ и ч. 1 ст. 274.1 УК РФ – двойную роль преступной цели и альтернативного последствия, хотя

некоторые авторы считают, что данный признак выполняет роль функционально-целевой характеристики преступного средства

Институту наказания в уголовно-правовой науке посвящено значительное число публикаций, которые регулярно пополняются новыми источниками, отражающими современные проблемы института наказания и авторское понимание мер уголовно-правового воздействия и их назначения судом.

В соответствии с положениями ст. 159.6 УК РФ, в настоящем исследовании нами рассмотрены возможные виды наказаний по соответствующим частям и пунктам с примерами из правоприменительной практики. Таким образом, следует вывод, что вид наказания за совершение преступлений, предусмотренных ч. 1, ч. 2, ч. 3, ч. 4 ст. 159.6 УК РФ может быть различным. Вид наказания избирается судом с учетом определенных сведений: степени и опасности преступного посягательства, наличие смягчающих и отягчающих обстоятельств, наличие судимости, характеристика по месту работы, жительства и учебы и много другое.

В заключение, необходимо сказать, что на сегодняшний день сфера преступлений в компьютерной информации – это живая, постоянно развивающаяся сфера общественных отношений, требующая уголовноправовой защиты. Очевидно, что изменения в данном вопросе ещё будут, поскольку даже сегодня существуют юридико-технические проблемы, проблемы несоответствия санкций смежных преступлений, проблемы недостаточного понимания правоприменителем объектов смежных составов.

Оценивая динамику на протяжении нескольких лет, можно с уверенностью сказать, что суды стараются выравнивать и решать ошибки законодателя, а законодатель обращает внимание на недостатки формулировок и старается их исправлять. Будем надеяться, что с учётом работы всех сфер государства, совершенствования уголовно-процессуальных

способов раскрытия и пресечения такого рода преступлений, в ближайшее время нам удастся поставить эту сферу под контроль и сделать максимально безопасной для законопослушного общества.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

I. Законы, нормативные правовые акты и иные официальные документы:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 01.07.2020 № 11-ФКЗ) // СЗ РФ. – 2020. – № 31. – Ст. 4398.

2. О персональных данных: Федеральный закон от 27.07.2006 №N 152-ФЗ // Справ.-правовая система «КонсультантПлюс» (дата обращения: 10.09.2023).

3. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ // Справ.-правовая система «КонсультантПлюс» (дата обращения: 10.09.2023).

4. Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления: Федеральный закон от 09.02.2009 № 8-ФЗ // Справ.-правовая система «КонсультантПлюс» (дата обращения: 10.09.2023).

5. Уголовно-исполнительный кодекс Российской Федерации: Федеральный закон от 08.01.1997 № 1-ФЗ // Справ.-правовая система «КонсультантПлюс» (дата обращения: 10.09.2023).

6. Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18.12.2001 № 174-ФЗ // Справ.-правовая система «КонсультантПлюс» (дата обращения: 10.09.2023).

7. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ // Справ.-правовая система «КонсультантПлюс» (дата обращения: 10.09.2023).

8. О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы: Указ Президента РФ от 09.05.2017 № 203 // Справ.-правовая система «КонсультантПлюс» (дата обращения: 10.09.2023).

II. Монографии, учебники, учебные пособия:

9. Бойко С.Я. Уголовная ответственность за мошенничество: теоретико-прикладное исследование. М.: Юрлитинформ, 2019. – 198 с.

10. Боровиков В. Б. Уголовное право. Особенная часть : учебник для среднего профессионального образования / В. Б. Боровиков, А. А. Смердов ; под редакцией В. Б. Боровикова. – 7-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2023. – 505 с.

11. Боровиков, В. Б. Уголовное право. Особенная часть : учебник для вузов / В. Б. Боровиков, А. А. Смердов ; под редакцией В. Б. Боровикова. – 7-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2023. – 505 с.

12. Коломинов В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дис. … канд. юрид. наук. – Иркутск, 2017. – С. 12.

13. Сверчков В. В. Уголовное право : учебник для среднего профессионального образования / В. В. Сверчков. – 10-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2023. – 727 с.

14. Сверчков В. В. Уголовное право. Общая и Особенная части : учебник для вузов / В. В. Сверчков. – 10-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2023. – 727 с.

15. Уголовная ответственность и наказание : учебное пособие для вузов / И. А. Подройкина [и др.] ; под редакцией И. А. Подройкиной. – 6-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2023. – 269 с.

16. Уголовное право России. Особенная часть : учебник для вузов / О. С. Капинус [и др.]. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 1189 с.

17. Уголовное право. Особенная часть : учебник для вузов / А. В. Наумов [и др.] ; ответственные редакторы А. В. Наумов, А. Г. Кибальник. – 5-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2023. – 499 с.

18. Уголовное право. Особенная часть. Краткий курс : учебное пособие для вузов / И. Я. Козаченко [и др.] ; ответственный редактор И. Я. Козаченко. – Москва : Издательство Юрайт, 2023. – 263 с.

19. Уголовное право. Особенная часть. Преступления в сфере экономики : учебник для вузов / В. И. Гладких [и др.] ; под общей редакцией В. И. Гладких, А. К. Есаяна. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2023. – 324 с.

III. Статьи, научные публикации:

20. Абдульмянова, Т. В. Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ): понятие, уголовно-правовая характеристика и некоторые особенности расследования / Т. В. Абдульмянова, И. П. Асанова, В. В. Данилов // Вопросы российского и международного права. – 2021. – Т. 11, № 1А. – С. 134-145. – DOI 10.34670/AR.2020.23.36.021.

21. Адашевский, Г. Мошенничество в сфере компьютерной информации: проблемы законодательной регламентации / Г. Адашевский // Уголовная политика и правоприменительная практика : Сборник материалов IX Международной научно-практической конференции, Санкт-Петербург, 11 марта 2022 года / Под общей редакцией Е.Н. Рахмановой. – Санкт-Петербург: Центр научно-информационных технологий "Астерион", 2022. – С. 646-654.

22. Алексеев, Д. С. Мошенничество в сфере компьютерной информации: особенности квалификации и конкуренции со смежными составами преступлений / Д. С. Алексеев // Аллея науки. – 2022. – Т. 1, № 2(65). – С. 508-518.

23. Алферова, Е. В. Назначение уголовного наказания: системные исследования российских ученых-специалистов в области уголовного права, уголовного процесса, уголовно-исполнительного права и криминологии / Е. В. Алферова // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Серия 4: Государство и право. – 2020. – № 1. – С. 123-130.

24. Бархатова, Е. Н. Мошенничество в сфере предпринимательства: теория, практика, проблемы / Е. Н. Бархатова, А. О. Миронов // Безопасность бизнеса. – 2021. – № 2. – С. 27-31. – DOI 10.18572/2072-3644-2021-2-27-31.

25. Борисов, А. В. О некоторых аспектах объекта мошенничества / А. В. Борисов // Военное право. – 2021. – № 4(68). – С. 264-269.

26. Бородин, А. В. Объективная сторона мошенничества, предусмотренного статьей 159.6 уголовного кодекса Российской Федерации / А. В. Бородин, М. В. Косолапов // Colloquium-Journal. – 2019. – № 16-7(40). – С. 25-26.

27. Власов, В. А. Отдельные актуальные правовые аспекты мошенничества с использованием компьютерной информации / В. А. Власов, В. А. Кондратова, И. В. Морозова // Аграрное и земельное право. – 2020. – № 11(191). – С. 159-162. – DOI 10.47643/1815-1329_2020_11_159.

28. Куликов, А. В. Мошенничество в сфере компьютерной информации / А. В. Куликов, Е. А. Гуц // Известия Тульского государственного университета. Экономические и юридические науки. – 2020. – № 1. – С. 81-88.

29. Лопашенко Н.А. Компьютерное мошенничество - новое слово в понимании хищения или ошибка законодателя? // Пермский юридический альманах. – 2019. – №2. – С. 598-608.

30. Рождайкина, Е. И. Особенности квалификации объекта и объективной стороны мошенничества в сфере компьютерной информации / Е. И. Рождайкина // Эволюция российского права : Материалы XIX Международной научной конференции молодых ученых и студентов, Екатеринбург, 29–30 апреля 2021 года / Уральский государственный юридический университет. – Екатеринбург: Федеральное государственное бюджетное образовательное учреждение высшего образования "Уральский государственный юридический университет", 2021. – С. 1276-1280.

31. Савельев И.В. Мошенничество в сфере компьютерной информации: потенции квалификационных страданий / И.В. Савельев // Вопросы российской юстиции. – 2019. – №4. – С. 436-452.

32. Степанов М. В. Критический анализ нормы о мошенничестве в сфере компьютерной информации (ст. 159.6 УК РФ). // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2019. – № 1 (33). – С. 173.

33. Хисамова, З. И. Об особенностях квалификации преступлений, совершаемых в сфере использования информационно-коммуникационных технологий / З. И. Хисамова // Общество и право. – 2021. – № 1(55). – С. 117-120.

34. Энгельгардт А.А. Вопросы квалификации мошенничества в сфере компьютерной информации. // Право. Журнал Высшей школы экономики. – 2020. – № 4. – С. 86.

IV. Эмпирические материалы:

35. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»:

Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 // Справ.-правовая система «КонсультантПлюс» (дата обращения: 29.12.2023).

36. О судебной практике по делам о мошенничестве, присвоении и растрате: Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 // Российская газета. – 2017. – № 280.

37. Апелляционное определение Томского областного суда от 12.10.2017 по делу № 22-1652/2017 // Справ.-правовая система «Консультант Плюс» (дата обращения: 07.10.2023).

38. Постановление Вахитовского районного суда г. Казани Республики Татарстан № 1-413/2020 от 29 июля 2020 г. по делу № 1-413/2020. URL: https://sudact.ru/regular/doc/ftR7s3xLHjHQ/ (дата обращения: 29.12.2023).

39. Постановление Девятого арбитражного апелляционного суда от 15 мая 2018 г. № 09АП16416/2018 по делу № А40-124668/2017. – URL: https://www.garant.ru (дата обращения: 20.10.2023).

40. Постановление Кудымкарского городского суда Пермского края по делу № 1-290/2018 от 20 декабря 2018 г. URL: https://clck.ru/37N3fy (дата обращения: 29.12.2023).

41. Постановление Сухиничского районного суда Калужской области по делу № 1-4-38/2021 от 16 апреля 2021 г. URL: https://clck.ru/37N3DL (дата обращения: 29.12.2023).

42. Приговор №1-1082/2022 от 30 июня 2022 г. по делу №1-1082/2022. URL: https://clck.ru/37N54J (дата обращения: 10.12.2023).

43. Приговор Димитровградского городского суда Ульяновской области от 22.08.2017. по делу №1-256/2017. URL: http://dimitrovgradskiy.uln.sudrf.ru/ (дата обращения: 29.12.2023).

44. Приговор Засвияжского районного суда г. Ульяновска по делу №1-376/2019 от 05 сентября 2019 года. URL: https://clck.ru/37N2ga (дата обращения: 29.12.2023).

45. Приговор Засвяженского районного суда г. Ульяновска по делу № 2-1/2018 // Ульяновский городской суд. – URL: http://zasvijajskiy.uln.sudrf.ru/ (дата обращения: 10.12.2023).

46. Приговор Мотовилихинского районного суда г. Перми по делу №1-72/2019 от 20 февраля 2019 г. URL: https://clck.ru/37N3Xj (дата обращения: 29.12.2023).

47. Приговор Октябрьского районного суда г. Владимира № 1-95/2019 от 4 июня 2019 г. по делу № 1-95/2019. – URL: https://sudact.ru/regular/doc/v59eyhN7lzJq/ (дата обращения: 07.10.2023)

48. Приговор Первомайского районного суда г. Владивостока от 02.06.2018 по уголовному делу № 2-2876/2018. // Архив Первомайского районного суда г. Владивостока. 2018. Д. 2876/2018. Л. Д. 225.

49. Приговор по ст. 159.6 УК РФ // Московский городской суд. – URL: https://mos-gorsud.ru/ (дата обращения: 20.10.2023).

50. Приговор Пушкинского районного суда г. Санкт-Петербурга от 4 апреля 2017 г. по делу № 1–74/2017. – URL: https://sudact.ru/regular/doc/KfAZx4gNIDNV/ (дата обращения: 07.10.2023).

51. Приговор Свердловского районного суда г. Белгорода. Дело № 1-64/2013. URL: https://sverdlovsky-blg.sudrf.ru (дата обращения: 07.10.2023).

52. Приговор Симоновского районного суда г. Москвы по делу № 1-79/2013 от 14 февраля 2013 г. // Справ.-правовая система «КонсультантПлюс» (дата обращения: 29.12.2023)

53. Приговор Советского районного суда г. Владивостока (Приморский край) № 1-277/2020 от 30 июля 2020 г. по делу № 1-277/2020. URL: https://sudact.ru/regular/doc/4AyuDmz7J9oX/ (дата обращения: 29.12.2023).

54. Приговор суда по ч. 2 ст. 159.6 УК РФ № 1-417/2017. URL: https://sud-praktika.ru/precedent/(дата обращения: 07.10.2023).

55. Приговор Фрунзенского районного суда г. Саратова № 1-66/2018 от 19 июля 2018 г. по делу № 1-66/2018. URL: https://sudact.ru/regular/doc/qtCZQWKOpk5x/ (дата обращения: 29.12.2023).

56. Приговор Центрального районного суда г. Кемерово по делу № 1-573/2020 от 08 сентября 2020 г. URL: https://clck.ru/37N49E (дата обращения: 29.12.2023).

57. Приговор Якутского городского суда (Республика Саха (Якутия)) № 1-681/2019 от 26 августа 2019 г. по делу № 1-1462/2018. URL: https://sudact.ru/regular/doc/8jIATe7oVfNK/ (дата обращения: 29.12.2023).

58. Приговоры судов по ст. 159.6 УК РФ Мошенничество в сфере компьютерной информации. Режим доступа: http://sud-praktika.ru/ (дата обращения: 29.12.2023).

59. Решение № 2А-7195/2020 2А-7195/2020~М-7803/2020 от 19 ноября 2020 г. по делу № 2А-7195/2020. URL: https://sudact.ru/regular/doc/ (дата обращения: 07.10.2023).

V. Справочная литература:

60. В Перми вынесен приговор виновному в серии преступлений в сфере телекоммуникаций и компьютерной информации. URL: https://59.xn--b1aew.xn--p1ai/news/item/15783318 (дата обращения: 07.10.2023).

61. В Тюмени будут судить жителя Перми за хищение 10,5 млн рублей с помощью вирусного ПО. URL: https://www.kommersant.ru/doc/4637386 (дата обращения: 07.10.2023).

АНТИПЛАГИАТ
ОБНАРУЖЕНИЕ ЗАИМСТВОВАНИЙ

СПРАВКА

о результатах проверки текстового документа
на наличие заимствований

Казанский юридический институт МВД России

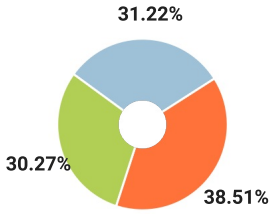
ПРОВЕРКА ВЫПОЛНЕНА В СИСТЕМЕ АНТИПЛАГИАТ.ВУЗ

Автор работы: Ялалов Данил Ильмирович
Самоцитирование рассчитано для: Ялалов Данил Ильмирович
Название работы: ВКР Ялалов
Тип работы: Выпускная квалификационная работа
Подразделение: Уголовное право

РЕЗУЛЬТАТЫ

СОВПАДЕНИЯ	38.51%
ОРИГИНАЛЬНОСТЬ	31.22%
ЦИТИРОВАНИЯ	30.27%
САМОЦИТИРОВАНИЯ	0%

ДАТА ПОСЛЕДНЕЙ ПРОВЕРКИ: 21.05.2024



Структура документа: Проверенные разделы: библиография с.60-67, титульный лист с.1, содержание с.2, основная часть с.3-59
Модули поиска: Перефразирования по СПС ГАРАНТ: аналитика; Цитирование; Медицина; Интернет Плюс; Переводные заимствования по eLIBRARY.RU (EnRu); eLIBRARY.RU; Переводные заимствования издательства Wiley (RuEn); СМИ России и СНГ; СПС ГАРАНТ: нормативно-правовая документация; Переводные заимствования (RuEn); Сводная коллекция вузов МВД; Библиография; ИПС Адилет; Сводная коллекция ЭБС; Модуль поиска "КЮИ МВД РФ"; Перефразирования по eLIBRARY.RU; Шаблонные фразы; Перефразирования по Интернету; СПС ГАРАНТ: аналитика; Переводные заимствования по Интернету (EnRu); Издательство Wiley; Патенты СССР, РФ, СНГ; Диссертации НББ; Кольцо вузов; Сводная коллекция РГБ

Работу проверил: Нурутдинов Ильнур Ильдусович

ФИО проверяющего

Дата подписи:

Подпись проверяющего

Чтобы убедиться в подлинности справки, используйте QR-код, который содержит ссылку на отчет.

Ответ на вопрос, является ли обнаруженное заимствование корректным, система оставляет на усмотрение проверяющего. Предоставленная информация не подлежит использованию в коммерческих целях.

ОТЗЫВ

о работе обучающегося 092 учебного взвода очной формы обучения,
2019 года набора по специальности
40.05.02 Правоохранительная деятельность
Ялалова Данила Ильмировича
в период подготовки дипломной работы
на тему «Уголовная ответственность за мошенничество в сфере компьютерной информации».

Выбор темы исследования «Уголовная ответственность за мошенничество в сфере компьютерной информации» слушателем был осуществлен из списка, предложенного кафедрой с учетом научных интересов и спецификой будущего направления профессиональной деятельности.

Данил Ильмирович в ходе работы показал наличие высокой заинтересованности в исследовательской деятельности, осуществлялись постоянные консультации, разбор и анализ предоставленного материала.

Предыдущие научные исследования, эмпирический материал по выбранной теме у слушателя отсутствуют.

Слушатель Ялалов проявляет умение корректно формулировать цели и ставить задачи (проблемы) своей деятельности при выполнении дипломной работы, анализировать, диагностировать причины появления проблем, их актуальность.

Слушатель самостоятельно разработал план исследования, который характеризуется логичностью и структурированностью.

Эмпирический материала по тематике дипломной работы был отобран и обобщен автором в разумные сроки.

Автор проявил инициативу и самостоятельность в выборе методов исследования, постановки цели и задач, способах описания результатов исследования, показал навыки в работе с материалами следственно-судебной практики, способность и умения анализа статистических данных и их

применения в исследовании.

Умение оперировать уголовно-правовыми терминами и категориями и их применение в процессе написания работы высокое. Данил Ильмирович проявляет способность к самостоятельному формулированию выводов и результатов исследования, пунктуальность в выполнении структурных элементов работы в установленные научным руководителем сроки.

Работу характеризует самостоятельные, обоснованные и достоверные выводы из проделанного исследования.

Дипломная работа Ялалова Данила Ильмировича на тему «Уголовная ответственность за мошенничество в сфере компьютерной информации» может быть допущена к защите и заслуживает положительной оценки.

Руководитель:
старший преподаватель кафедры уголовного права
Казанского юридического института МВД России
кандидат социологических наук
подполковник полиции И.И. Нурутдинов
«22» мая 2024г.

С отзывом ознакомлен Д.И. Ялалов
«22» мая 2024г.

РЕЦЕНЗИЯ

на дипломную работу
обучающегося 092 учебного взвода очной формы обучения,
2019 года набора по специальности
40.05.02 Правоохранительная деятельность
Ялалова Данила Ильмировича
на тему «Уголовная ответственность за мошенничество в сфере компьютерной информации».

Выбор темы исследования полностью обоснован автором. Цель и задачи работы сформулированы точно. Название дипломной работы, цель и задачи полностью соответствуют содержанию работы.

Работа состоит из двух глав (Уголовно-правовая характеристика мошенничества в сфере компьютерной информации; Уголовная ответственность за мошенничество в сфере компьютерной информации). Присутствует взаимосвязь между структурными частями работы, теоретическим и практическим содержанием. Структура дипломной работы соответствует целям и задачам, части работы соразмерны.

Работа написана на достаточном научном уровне, использован широкий спектр источников литературы, имеются правильные и обоснованные выводы. Автор анализирует мнения различных ведущих ученых, научных взглядов, приводит обоснованные и аргументированные выводы и предложения по работе.

Слушатель изучил основные теоретические работы, посвященных проблеме дипломной работы, провел сравнительно-сопоставительный анализ источников, и на основании этого определил и обосновал собственную позицию исследования.

Выводы работы логичны и обоснованы, полностью соответствуют целям и задачам работы.

В работе автор демонстрирует самостоятельность в подборе и анализе литературы, оригинальность текста, самостоятельность сделанных обобщений, наличие и обоснованность теоретических выводов и предложений по совершенствованию уголовного законодательства России.

В работе имеются достаточные и достоверные практические материалы, примеры судебной практики по исследуемому вопросу, обоснование и интерпретация слушателем полученных эмпирических результатов. Результат исследования может быть эффективно использован в практической деятельности правоохранительных органов.

Слушатель демонстрирует знание нормативно-правовых актов, профессиональной литературы, источников, фундаментальных исследований по теме, публикаций ведущих специалистов в области темы исследования что положительно сказывается на качестве работы.

Дипломная работа изложена научным стилем. Работа оформлена в соответствии с предъявляемыми требованиями (правильное оформление отдельных элементов текста - абзацев текста, заголовков, формул, таблиц, рисунков - и ссылок на них; соблюдение уровней заголовков и подзаголовков; наличие в тексте ссылок на работы и источники, указанные в списке литературы, библиографических ссылок, списка литературы и нормативно-правовых актов, аккуратность исполнения).

Дипломная работа Ялалова Данила Ильмировича на тему «Уголовная ответственность за мошенничество в сфере компьютерной информации» может быть допущена к защите и заслуживает оценку «отлично».

Оценка рецензента: отлично

Рецензент

ВРИО заместителя начальника ОП №4 «Электротехнич/с

УМВД России по г. Набережные Челны

подполковник полиции Р.Р. Идиятуллин

« »

С рецензией ознакомлен Д.И. Ялалов