На правах рукописи

Фролов Михаил Дмитриевич

УГОЛОВНО-ПРАВОВОЕ И КРИМИНОЛОГИЧЕСКОЕ ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСТВУ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Специальность 12.00.08 — Уголовное право и криминология;
уголовно-исполнительное право

Автореферат
диссертации на соискание ученой степени
кандидата юридических наук

Москва — 2019

Диссертация выполнена на кафедре уголовного права, уголовного процесса и криминалистики Федерального государственного автономного образовательного учреждения высшего образования «Российский университет дружбы народов».

Научный руководитель: **Букалерова Людмила Александровна,**
доктор юридических наук, профессор

Официальные оппоненты: **Трунцевский Юрий Владимирович,**
доктор юридических наук, профессор,
ведущий научный сотрудник отдела
методологии противодействия коррупции
ФГНИУ «Институт законодательства
и сравнительного правоведения при
Правительстве Российской Федерации»

Чупрова Антонина Юрьевна,
доктор юридических наук, профессор,
профессор кафедры уголовного права
и криминологии ФГБОУ ВО «Всероссийский
государственный университет юстиции
(РПА Минюста России)»

Ведущая организация: Федеральное государственное казенное
образовательное учреждение высшего
образования «Московский университет
Министерства внутренних дел Российской
Федерации имени В.Я. Кикотя»

Защита состоится «18» апреля 2019 г. в 14.00 часов на заседании диссертационного совета Д 212.203.24 при ФГАОУ ВО «Российский университет дружбы народов» по адресу: 117198, г. Москва, ул. Миклухо-Маклая, д. 6, ауд. № 347, зал заседаний Ученого совета.

С диссертацией можно ознакомиться в Научной библиотеке и на официальном сайте Федерального государственного автономного образовательного учреждения высшего образования «Российский университет дружбы народов» по адресу: http://dissovet.rudn.ru.

Автореферат разослан «____» _____ 2019 г.

Ученый секретарь диссертационного совета
кандидат юридических наук О. А. Кузнецова

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Мошенничество можно отнести к числу так называемых традиционных составов преступлений, достаточно хорошо изученных в науке уголовного права. Однако построение «цифровой экономики» в XXI в. вкупе с удешевлением средств автоматизированной обработки (передачи) данных и экспонентным ростом числа пользователей современными компьютерными технологиями открыл новые возможности для представителей криминального мира. Как следствие, виды и способы мошенничества быстро и существенно трансформируются, придавая ему все большее виртуальное измерение.

Использование информационно-телекоммуникационных технологий в преступных целях в последние годы является серьезным вызовом как для правоохранительных, так и законодательных органов. Выступая на цифровом форуме в Сеуле, Генеральный секретарь ООН Пан Ги Мун отметил, что революция в области информационно-коммуникационных технологий сопровождается новыми угрозами, связанными с киберпреступностью[1].

Федеральным законом от 29 ноября 2012 г. Уголовный кодекс Российской Федерации был дополнен шестью новыми нормами о мошенничестве, одной из которых стала ст. 159.6 «Мошенничество в сфере компьютерной информации». С точки зрения интеграции российского законодательства о борьбе с преступлениями в сфере компьютерной информации в международное законодательство такой шаг является закономерным и обоснованным. Фактически с включением ст. 159.6 УК РФ в национальное законодательство разрешен вопрос о полноправной интеграции Российской Федерации в мировую систему противодействия преступности в сфере информационных технологий (киберпреступности). Однако специальное выделение мошенничества в сфере компьютерной информации породило и ряд проблем, связанных как с толкованием, так и с применением данной нормы. Не все из них разрешены и в новом постановлении Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате».

Мошенничество в сфере компьютерной информации обладает своей спецификой, имеет транснациональный масштаб, постоянно изменяет свои формы, высоколатентно и, как следствие, с трудом поддается имеющимся мерам противодействия. Так, при общем росте мошенничеств в целом в 2016 г. их зарегистрировано 208,9 тыс., а в 2017 г. — 222,8 тыс.; количество лиц, осужденных по ст. 159.6 УК РФ, сравнительно невелико. По данным Судебного департамента при Верховном Суде РФ, в 2016 г. по всем статьям о мошенничестве было осуждено 23 705 человек и только 124 человека по ст. 159.6 УК РФ (8 — по ч. 1 ст. 159.6 УК РФ, 81 — по ч. 2, 17 — по ч. 3 и 18 —

[1] Официальный сайт ООН. URL: http://www.un.org/russian/news/story.asp?NewsID=23769#.VY5a1psdCt8 (дата обращения: 18.10.2017).

по ч. 4), в 2017 г. из 23 044 осужденных по всем статьям о мошенничестве всего 144 по ст. 159.6 УК РФ (14 — по ч. 1 ст. 159.6 УК РФ, 68 — по ч. 2, 20 — по ч. 3 и 42 — по ч. 4)[2].

Обращение к обозначенной проблеме объясняется необходимостью разработать инструменты и механизмы, обеспечивающие эффективное уголовно-правовое противодействие мошенничеству в сфере компьютерной информации, с учетом проблемы трансграничной юрисдикции независимо от территории, с которой совершено преступление, и (или) местонахождения, а также постоянно усложняющихся применяемых технических средств.

Кроме того, требуют обстоятельного научного анализа и оценки весьма противоречивые изменения, внесенные в ст. 159.6 УК РФ Федеральным законом от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений и дополнений в Уголовный кодекс Российской Федерации».

В свете изложенного своевременной видится постановка вопроса о необходимости проведения всестороннего исследования комплекса теоретических и практических проблем уголовной ответственности за мошенничество в сфере компьютерной информации, а также основных направлений и мер его предупреждения на общесоциальном и специально-криминологическом уровнях.

Степень научной разработанности темы. Мошенничество становилось предметом научного анализа в работах многих авторов. Его исследованию посвящены труды И. А. Александровой, И. Р. Бегишева, А. Г. Безверхова, В. И. Гладких, М. Ю. Дворецкого, К. Н. Евдокимова, В. М. Елина, М. А. Ефремовой, Л. Р. Клебанова, Н. Ш. Козаева, В. Ю. Окружко, М. А. Простосердова, А. А. Пудовкина, Е. А. Русскевича, О. М. Сафонова, С. В. Склярова, Д. О. Тепловой, М. И. Третьяк, Н. А. Чикишевой, А. А. Шутовой, А. А. Южина, С. В. Ямашкина и др.

Специальных исследований, посвященных проблемам уголовно-правового противодействия мошенничеству в сфере компьютерной информации в теории российского уголовного права не так уж много. Так, можно выделить кандидатские диссертации С. С. Медведева «Мошенничество в сфере высоких технологий»[3] и А. А. Комарова «Криминологические аспекты мошенничества в глобальной сети Интернет»[4].

В 2016 году сразу в двух кандидатских диссертациях частично рассматривались вопросы уголовно-правового противодействия компьютерному мошенничеству. Это работы А. А. Южина «Мошенничество и его виды

---

[2] Официальный сайт Судебного департамента при Верховном Суде РФ. URL: http://cdep.ru/index.php?id=79&item=3832 (дата обращения: 26.07.2018).

[3] *Медведев С. С.* Мошенничество в сфере высоких технологий : дис. канд. юрид. наук : 12.00.08. Краснодар, 2008. 210 с.

[4] *Комаров А. А.* Криминологические аспекты мошенничества в глобальной сети Интернет. : дис. канд. юрид. наук : 12.00.08. Пятигорск, 2011. 262 с.

в российском уголовном праве» [5] и М. А. Простосердова «Экономические преступления, совершаемые в киберпространстве, и меры противодействия им»[6].

Проблематика мошенничества в сфере компьютерной информации получила свое освещение также в двух докторских диссертациях, авторами которых являются Н. Ш. Козаев «Современные проблемы уголовного права, обусловленные научно-техническим прогрессом»[7] и М. А. Ефремова «Уголовно-правовая охрана информационной безопасности»[8].

Исследования, проведенные этими и другими авторами, без сомнения, внесли значительный вклад в разработку проблемы уголовно-правового противодействия мошенничеству в сфере компьютерной информации. Вместе с тем до настоящего времени в отечественной юридической науке остается нерешенным целый ряд вопросов, связанных с пониманием и применением ст. 159.6 УК РФ. Так, не выработано общепринятое понимание отдельных признаков преступления, предусмотренного данной уголовно-правовой нормой, не исследованы его квалифицированные виды, остались не раскрытыми многие проблемные вопросы его квалификации и др.

Отдельно необходимо отметить, что более ранние исследования по понятным причинам не предполагали критического анализа самой конструкции ст. 159.6 УК РФ, а также объективно были лишены возможности обстоятельного обобщения и анализа правоприменительной практики по данной статье.

Целью диссертационного исследования является комплексный анализ норм отечественного, международного и зарубежного законодательства об ответственности за мошенничество в сфере информации и разработка научно обоснованных рекомендаций и предложений по преодолению проблем, возникающих в связи уголовно-правовым и криминологическим противодействием преступлениям в данной сфере.

Реализация сформулированной цели обусловила необходимость постановки и последовательного решения следующих **задач:**

- изучить международно-правовые стандарты и основные подходы к регламентации уголовной ответственности за мошенничество в сфере компьютерной информации, используемые в законодательстве зарубежных стран;
- определить социально-правовые основания криминализации мошенничества в сфере компьютерной информации;
- осуществить полный юридический анализ состава преступления, предусмотренного ст. 159.6 УК РФ;
- выявить недостатки уголовного законодательства об ответственности за совершение преступления, предусмотренного ст. 159.6 УК РФ;

---

[5] *Южин А. А.* Мошенничество и его виды в российском уголовном праве : дис. канд. юрид. наук : 12.00.08. М., 2016. 238 с.

[6] *Простосердов М. А.* Экономические преступления, совершаемые в киберпространстве, и меры противодействия им : дис. канд. юрид. наук : 12.00.08. М., 2016. 232 с.

[7] *Козаев Н. Ш.* Современные проблемы уголовного права, обусловленные научно-техническим прогрессом : дис. д-ра юрид. наук : 12.00.08. Краснодар, 2017. 630 с.

[8] *Ефремова М. А.* Уголовно-правовая охрана информационной безопасности : дис. д-ра юрид. наук : 12.00.08. М., 2018. 427 с.

- проанализировать практику применения ст. 159.6 УК РФ с целью выявления и устранения имеющихся трудностей и ошибок;

- разработать рекомендации по квалификации преступления, предусмотренного ст. 159.6 УК РФ, и его отграничению от смежных составов преступлений в следственной и судебной практике;

- сформулировать предложения по совершенствованию конструкции состава преступления, предусмотренного ст. 159.6 УК РФ;

- разработать предложения по предупреждению мошенничества в сфере компьютерной информации.

Объектом исследования является сфера общественных отношений, возникающих в связи с законодательным закреплением и практической реализацией уголовно-правовой нормы об ответственности за мошенничество в сфере компьютерной информации.

Предметом исследования выступают непосредственно уголовно-правовая норма, регламентирующая ответственность за мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), а также соответствующие нормы зарубежного уголовного законодательства; материалы судебно-следственной практики; криминогенные факторы преступления, предусмотренного ст. 159.6 УК РФ; личность компьютерного мошенника; конкретные меры предупреждения мошенничества в сфере компьютерной информации; научные работы по исследуемой проблематике и результаты социологических исследований.

Нормативная база исследования представлена источниками международного и национального права России и зарубежных стран. В их числе: Конституция Российской Федерации, Уголовный кодекс Российской Федерации, федеральные законы от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе», от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации» и мн. др.

Теоретическую основу исследования составляют основные положения доктрины российского уголовного права, а также относящиеся к объекту исследования труды в области криминологии, международного права, теории права и государства, уголовного права, социологии и др. При проведении исследования использовались работы Г. Н. Борзенкова, Б. В. Волженкина, Л. Д. Гаухмана, В. И. Гладких, М. А. Ефремовой, А. Э. Жалинского, И. В. Ильина, И. В. Иногамовой-Хегай, И. А. Клепицкого, С. М. Кочои, Г. А. Кригера, Н. А. Лопашенко, А. В. Наумова, Ю. Е. Пудовочкина, В. Г. Степанова-Егинянца, И. Я. Фойницкого, В. В. Хилюты, А. Ю. Чупровой, П. С. Яни и др.

Эмпирическая база исследования включает:

- статистические данные о применении ст. 159.6 УК РФ за 2012–2018 гг.;

- материалы 165 уголовных дел о мошенничестве в сфере компьютерной информации;

- результаты анкетирования и интервьюирования: а) 52 служащих кредитных организаций и индивидуальных предпринимателей г. Москвы, Московской, Владимирской, Тверской, Тульской областей, Ставропольского края и Республики Татарстан; б) практических работников г. Москвы, Московской, Владимирской, Тверской, Тульской областей, Ставропольского края и Республики Татарстан: 26 судей федеральных судов общей юрисдикции и мировых судей, 37 прокуроров и помощников прокуроров, 42 практикующих адвокатов, 53 следователей, дознавателей и оперативных сотрудников по проблемам практической реализации ст. 159.6 УК РФ; в) 43 докторов и кандидатов юридических наук по основным теоретическим аспектам, связанным с проблемами правовой регламентации и практической реализации уголовно-правовой нормы об ответственности за мошенничество в сфере компьютерной информации; г) 67 граждан;

- результаты изучения материалов уголовных дел и опроса правоприменителей, приведенные другими исследователями;

- аналитические материалы, опубликованные в печатных СМИ и интернет-изданиях, таких как «Российская газета», «Ведомости», «Коммерсантъ», «РосБизнесКонсалтинг», «Экономика и жизнь», «Экономика и предпринимательство» и др.

Сбор и обработка эмпирических данных, положенных в основу исследования, осуществлялись с 2010 по 2018 гг.

Научная новизна диссертационного исследования заключается в том, что настоящая работа представляет собой одно из первых комплексных исследований мошенничества в сфере компьютерной информации и обусловлена современными потребностями, использованием новых идей и тенденций в области исследования общественных отношений, возникающих в связи с законодательным закреплением и практической реализацией уголовно-правовой нормы об ответственности за мошенничество в сфере компьютерной информации.

Кроме того, новизной обладают: а) положения, ставшие результатом актуального и комплексного анализа международного и зарубежного уголовного законодательства об ответственности за мошенничество в сфере компьютерной информации; б) предложения по разрешению дискуссионных вопросов, связанных с содержанием криминообразующих признаков состава преступления, предусмотренного ст. 159.6 УК РФ; в) авторское толкование его квалифицированных видов; г) рекомендации по проблемным вопросам квалификации мошенничества в сфере компьютерной информации в аспекте уголовно-правовых институтов соучастия, неоконченного преступления и множественности; д) предложения по совершенствованию действующего уголовного законодательства и правоприменительной практики по делам о мошенничестве в сфере компьютерной информации; е) рекомендации по предупреждению совершения преступления, предусмотренного ст. 159.6 УК РФ.

Теоретическая и практическая значимость работы заключается в том, что содержащиеся в диссертации выводы и предложения сориентированы на усиление противодействия мошенничеству в сфере компьютерной информации, а также в дополнении и развитии отечественной доктрины уголовного права, а именно ее разделов о преступлениях против собственности и в сфере компьютерной информации.

Практическое значение исследования состоит в его направленности на решение актуальных проблем отечественного законодательства, а также в возможности использования его выводов и предложений как в правотворческой и практической деятельности правоохранительных органов и суда, так и в учебном процессе при преподавании курсов «Криминология», «Уголовное право» и «Информационное право» и для повышения квалификации сотрудников правоохранительных органов и судей.

Методологическую основу исследования составляют общенаучный диалектический метод познания, а также частнонаучные методы: формально-логический, сравнительно-правовой, системно-структурный, социологический (анкетирование и интервьюирование) и некоторые другие.

В ходе исследования автором с использованием библиотечных ресурсов, в том числе электронных ресурсов ведущих индексов научного цитирования Web of Science и Scopus, официальных сайтов органов власти, был произведен отбор, изучение, обобщение и анализ научных публикаций, нормативных правовых актов, правоприменительной практики и официальной статистики по тематике исследования. Изучение международного опыта проводилось на основании компаративного анализа — для выявления уровня развития механизма уголовно-правовой защиты от мошенничества в сфере компьютерной информации с целью оценки перспектив имплементации положительных правовых технологий в законодательство Российской Федерации.

Для определения потенциального негативного влияния последствий мошенничества в сфере компьютерной информации, а также оценки уровня его опасности было проведено социологическое исследование, где респондентам предлагалось ответить на вопросы специально разработанной анкеты. В анкетировании и интервьюировании приняли участие не только практикующие специалисты в области юриспруденции, обеспечения информационной безопасности, но и независимые респонденты. Результаты опросов были систематизированы и сведены в соответствующие таблицы и графики. Полученные результаты позволяют оценить адекватность реакции со стороны государства на потребности общества в защите от мошенничества в сфере компьютерной информации.

Основные результаты диссертационного исследования репрезентативно представлены в следующих **положениях, выносимых на защиту:**

1. В целях обеспечения эффективного уголовно-правового противодействия мошенничеству в сфере компьютерной информации, с учетом проблемы трансграничной юрисдикции независимо от территории, с которой совершено преступление, и (или) местонахождения, а также постоянно усложняющихся

технических средств сформулированы наиболее перспективные направления совершенствования международно-правового механизма противодействия данному преступлению, которые включают в себя:

а) активизацию деятельности по продвижению в рамках ООН Конвенции об обеспечении международной информационной безопасности, а также разработке нового универсального документа взамен Конвенции Совета Европы о киберпреступности 2001 г. (Будапештской конвенции), взяв за основу концепцию Конвенции об обеспечении международной информационной безопасности, предложенной Российской Федерацией;

б) присоединение к созданной на саммите ЕС-США в ноябре 2010 г. Рабочей группе ЕС-США по кибербезопасности и киберпреступности (EU-US Working Group on Cyber Security and Counteracting Cybercrime) и поддержание идеи создания американо-российской группы по кибербезопасности, предложенной на саммите «Большой двадцатки» (G20).

2. Выявлены характерные особенности законодательств зарубежных стран в части уголовно-правовой регламентации ответственности за мошенничество в сфере компьютерной информации:

а) характеризуются весьма общим определением компьютерного мошенничества — как действия, совершаемого с компьютерной информацией с корыстной целью, причинившего вред собственнику или иному владельцу имущества;

б) критериями дифференциации ответственности являются: размер похищенного имущества, групповой характер совершения преступления, использование лицом своего доверительного (служебного) положения, использование информационно-телекоммуникационной сети «Интернет», сопряженность хищения с изменением, уничтожением или блокированием компьютерной информации, малолетний или престарелый возраст потерпевшего;

в) преобладающими видами наказания выступают штраф и лишение свободы (в зависимости от отсутствия или наличия отягчающих обстоятельств, срок варьируется от нескольких месяцев до 10 лет).

3. Основным непосредственным объектом мошенничества в сфере компьютерной информации выступают охраняемые уголовным законом общественные отношения в сфере собственности. При этом в качестве дополнительного объекта выступают общественные отношения, обеспечивающие информационную безопасность. Данное авторское уточнение содержания объекта мошенничества в сфере компьютерной информации сформулировано с учетом разъяснений Пленума Верховного Суда РФ, изложенных в постановлении от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»,

4. Разработаны следующие рекомендации по квалификации мошенничества в сфере компьютерной информации:

а) дано разъяснение признаков основного состава преступления, предусмотренного ст. 159.6 УК РФ, и его квалифицированных видов;

б) раскрыты особенности юридической оценки неоконченного мошенничества в сфере компьютерной информации, а равно совершенного в соучастии;

в) выделены и обоснованы критерии отграничения мошенничества в сфере компьютерной информации от смежных составов преступлений.

5. Аргументирована необходимость внесения изменений и дополнений в постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»:

а) абзац 2 пункта 20 изложить в следующей редакции: «По смыслу закона мошенничество в сфере компьютерной информации не требует дополнительной квалификации по статье 272 УК РФ. В случаях, когда лицо совершило хищение посредством создания, использования и распространения вредоносных компьютерных программ, содеянное необходимо квалифицировать по статье 159.6 УК РФ и статье 273 или 274.1 УК РФ»;

б) дополнить пункт 21 абзацем следующего содержания: «Когда хищение совершается путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным с последующим удалением, модификацией либо блокированием охраняемой законом компьютерной информации (например, лицо сначала по чужим данным заходит в личный кабинет клиента банка в сети «Интернет», осуществляет перевод денежных средств, и только потом меняет настройки доступа), содеянное требует дополнительной квалификации по статье 272 УК РФ».

6. Обоснован вывод о необходимости изменения системы квалифицирующих признаков мошенничества в сфере компьютерной информации. В частности, предлагается исключить п. «в» из ч. 3 ст. 159.6 УК РФ («с банковского счета, а равно в отношении электронных денежных средств»), введенный Федеральным законом от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации», — как противоречащий научно обоснованным критериям дифференциации уголовной ответственности.

7. Разработана авторская редакция уголовно-правовой нормы, предусмотренной ст. 159.6 УК РФ:

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

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

наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до трех лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до трех лет.

2. То же деяние, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину, а равно лицом, на которое по службе или работе возложены обязанности по обеспечению эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, либо с неправомерным доступом к охраняемой законом компьютерной информации, -

наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до пяти лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до одного года или без такового, либо лишением свободы на срок до пяти лет с ограничением свободы на срок до одного года или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные лицом с использованием своего служебного положения, а равно в крупном размере, -

наказываются штрафом 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, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового, либо лишением свободы на срок до семи 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.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, совершенные организованной группой либо в особо крупном размере, -

наказываются лишением свободы на срок до двенадцати 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».

8. Доказано, что система криминогенных детерминант мошенничества в сфере компьютерной информации включает: а) низкий уровень культуры информационной безопасности населения; б) недостаточный объем финансирования программ по развитию систем защиты платежных операций; в) просчеты в системе подбора и расстановки кадров кредитных организаций и компаний, оказывающих телематические услуги и услуги сетей передачи данных, также лиц, осуществляющих деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети «Интернет»; г) ограниченные функциональные возможности отделов собственной безопасности кредитных организаций и их слабое взаимодействие с правоохранительными органами; д) несовершенство регулятивного

законодательства в сфере трудовых отношений, информационной безопасности и электронной коммерции; е) низкая эффективность применения уголовно-правовых норм с двойной превенцией, а именно ст.ст. 272, 273, 274 и 274.1 УК РФ.

9. В целях предупреждения мошенничества в сфере компьютерной информации и эффективной превентивной стратегии предлагается комплекс мер общесоциального и специально-криминологического характера, который включает в себя: а) организационно-техническое ограничение анонимности пользователей в сети «Интернет», предполагающее обязательную идентификацию лишь в случаях, предусмотренных федеральным законом (например, при регистрации в социальных сетях, размещении объявлений о продаже товаров и оказании услуг); б) проведение на основе взаимодействия государственных органов, отраслевых структур и общественных организаций мониторинга информационных ресурсов на предмет обнаружения угроз, связанных с распространением сведений о неизвестных правоохранительным органам методах и способах компьютерного мошенничества, в целях дальнейшего блокирования данных ресурсов; в) повышение эффективности применения уголовно-правовых норм с двойной превенцией, предусмотренных ст.ст. 272, 273, 274 и 274.1 УК РФ; г) установление в ТК РФ нормативно закрепленных ограничений на осуществление трудовой деятельности в кредитно-финансовой сфере, а также в иных сферах на должностях, связанных с эксплуатацией и обслуживанием информационных (информационно-коммуникационных) технологий, лицам, ранее привлекавшимся к ответственности по ст. 159.6 УК РФ.

Степень достоверности и апробация результатов исследования. Основные теоретические положения и отдельные выводы автора обсуждались на заседаниях кафедры уголовного права, уголовного процесса и криминалистики РУДН, нашли свое отражение в 9 опубликованных работах автора (6 из которых — в изданиях, рекомендованных ВАК при Минобрнауки России), а также докладах и выступлениях автора на: Межвузовском научно-методическом семинаре «Научно-методическое обеспечение подготовки сотрудников внутренних дел в целях противодействия преступности», посвященном 20-летию принятия УК РФ (МосУ МВД России, г. Руза, 2016 г.); круглых столах «Квалификация преступлений: общие и частные проблемы» (Академия Генпрокуратуры РФ, г. Москва, 2016, 2017 гг.); Международной научно-практической конференции «Уголовное наказание в России и за рубежом: проблемы назначения и исполнения», посвященной 10-летию принятия Европейских пенитенциарных правил (Вологодский институт права и экономики ФСИН, Вологда, 2017 г.); Всероссийской научно-практической конференции «Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений» (Воронежский институт МВД России, Воронеж, 26 апреля 2018 г.), Всероссийской научной конференции «Уголовное право и информатизация преступности» (МосУ МВД России им. В. Я. Кикотя, Москва, 25–26 мая 2018 г.).

Структура диссертации. Работа состоит из введения, трех глав, объединяющих восемь параграфов, заключения и списка использованных источников.

СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во **введении** обосновывается актуальность темы исследования, определяются его цели и задачи, объект и предмет, анализируется степень научной разработанности темы, раскрываются теоретическая, нормативная, эмпирическая и методологическая основы, обосновывается научная новизна, формулируются основные положения, выносимые на защиту, определяется теоретическая и практическая значимость работы, приводятся сведения об апробации результатов и структуре исследования.

Первая глава «Международно-правовые стандарты и компаративный анализ уголовно-правового противодействия мошенничеству в сфере компьютерной информации» состоит из двух параграфов.

В первом параграфе «Международно-правовые стандарты противодействия мошенничеству в сфере компьютерной информации автор констатирует, что эффективное международное сотрудничество является ключевым условием успешного противодействия не только мошенничеству в сфере компьютерной информации, но и киберпреступности в целом. Только путем совместной работы государств и международных организаций по разработке универсальных механизмов контроля и управления информационно-коммуникационными технологиями можно обеспечить надлежащий уровень информационной безопасности, которая в настоящее время представляется труднодостижимой целью. В этой связи предлагается два основных направления международно-правового обеспечения противодействия мошенничеству в сфере компьютерной информации: а) посредством подготовки и принятия документов с целью гармонизации уголовных законодательств государств и б) путем принятия актов, направленных на предупреждение мошеннических действий в области электронной торговли.

Анализируя ряд международных актов, автор подчеркивает, что идея о необходимости уголовно-правового противодействия компьютерному мошенничеству в целом получила всеобщее признание. При этом рекомендательный характер международных соглашений позволяет государствам руководствоваться так называемым сбалансированным правовым подходом, который предусматривает, с одной стороны, самостоятельную криминализацию деяний против конфиденциальности, целостности и доступности компьютерных данных и компьютерных систем, а с другой — возможность применять к деяниям, совершенным с использованием информационно-коммуникационных технологий, уже имеющиеся положения об общеуголовных преступлениях, в том числе положения об ответственности за мошенничество.

Установлено, что под мошенничеством с использованием компьютерных технологий на уровне норм международного права в подавляющем большинстве случаев понимаются любые по характеру действия, связанные с изменением компьютерных данных, либо вмешательством в функционирование компьютерной системы, повлекшие лишение другого лица его собственности. В связи с этим автор указывает, что, несмотря на названия статей

соответствующих документов, с точки зрения отечественного законодательства речь в них идет не столько о мошенничестве, сколько о хищении в принципе, понятие которого раскрывается в примечании 1 к ст. 158 УК РФ.

По мнению диссертанта, нормы международного права не содержат каких-либо специальных требований (конкретных рекомендаций) относительно уголовной политики государств в части конструирования санкций за мошенничество в сфере компьютерной информации. Определяя общие признаки анализируемого преступления, отдельные международные акты (например, Конвенция «О преступности в сфере компьютерной информации» 2001 г.) указывают лишь на то, что к физическим лицам, совершившим преступление в сфере информационно-коммуникационных технологий, в том числе компьютерное мошенничество, должны применяться эффективные, соразмерные и убедительные наказания, включая лишение свободы.

Автор резюмирует, что отсутствие универсального международного инструмента, регулирующего противодействие преступлениям в сфере информационно-коммуникационных технологий, негативно сказывается на достижении гармонизации уголовного и уголовно-процессуального законодательства современных государств. Единственно верным решением данной проблемы является принятие международного акта по обеспечению кибербезопасности на базе Организации Объединенных Наций.

Во втором параграфе «Сравнительно-правовой анализ уголовного законодательства зарубежных стран об ответственности за мошенничество в сфере компьютерной информации» отмечается, что в связи с активным распространением новых информационных методов совершения мошенничества многие государства (в большинстве своем развитые) предприняли соответствующие меры по изменению (актуализации) национального уголовного законодательства.

В современных условиях уголовно-правовое противодействие компьютерному мошенничеству реализуется, как правило, путем: а) применения общих (традиционных) норм об общеуголовном мошенничестве; б) закрепления использования информационных технологий в качестве квалифицирующих признаков общей нормы о мошенничестве; в) создания ссылочных норм, устанавливающих ответственность за использование компьютерных технологий (информации) в целях совершения ряда преступлений, в том числе и мошенничества; г) регламентации специальной нормы о хищении с использованием компьютерной информации; д) путем законодательного определения специальной нормы о компьютерном мошенничестве.

На основе анализа зарубежного законодательства автор констатирует, что общепринятой практикой является весьма общее определение компьютерного мошенничества — как действия, совершаемого с компьютерной информацией с корыстной целью (при этом правомерность или неправомерность доступа к компьютерным данным значения не имеет), причинившего вред собственнику или иному владельцу имущества. Очевидно, что такой подход не в полной мере соответствует отечественному и традиционно сложившемуся пониманию

природы мошенничества, суть которого, как известно, заключается в воздействии на психику человека, введении его в заблуждение путем обмана или злоупотребления доверием, в результате чего виновный и завладевает имуществом.

Установлено, что в зависимости от распространенности критериями дифференциации уголовной ответственности за мошенничество в сфере компьютерной информации являются: а) размер похищенного имущества; б) групповой характер его совершения (в составе группы лиц по предварительному сговору или организованной группы); в) использование лицом своего доверительного (служебного) положения; г) использование информационно-телекоммуникационной сети «Интернет»; д) сопряженность хищения с изменением, уничтожением или блокированием компьютерной информации; е) малолетний или престарелый возраст потерпевшего.

Оригинальным подходом некоторых стран (например, Новой Зеландии) является установление ответственности за мошеннические действия в сфере компьютерной информации путем регламентации усеченного состава преступления, момент окончания которого связан не с появлением у виновного реальной возможности распоряжаться чужим имуществом (obtains any property), а с совершением определенных действий с компьютерной информацией в целях завладения чужим имуществом (to obtain any property).

Выявлено, что преобладающими видами наказания за компьютерное мошенничество выступают штраф и лишение свободы. При этом в зависимости от отсутствия или наличия отягчающих обстоятельств срок наказания в виде лишения свободы варьируется от нескольких месяцев до 10 лет.

По мнению диссертанта, практически полное отсутствие в уголовных законодательствах стран СНГ специальных норм о мошенничестве в сфере компьютерной информации во многом обусловлено влиянием принятого в 2001 г. Соглашения о сотрудничестве государств — участников СНГ в борьбе с преступлениями в сфере компьютерной информации, в котором такой состав отдельно не выделялся. Вместе с тем не только Россия, но и некоторые другие страны Содружества (Армения и Белоруссия) внесли изменения в свои уголовные кодексы с целью специального определения ответственности за хищение с использованием компьютерной информации.

Вторая глава «Юридический анализ мошенничества в сфере компьютерной информации по Уголовному кодексу Российской Федерации» содержит три параграфа.

В первом параграфе «Объективные признаки мошенничества в сфере компьютерной информации», подробно исследуя объективные признаки данного вида мошенничества, автор обосновывает вывод о том, что основным непосредственным объектом мошенничества в сфере компьютерной информации являются охраняемые уголовным законом общественные отношения в сфере собственности. В качестве факультативного объекта выступают общественные отношения, обеспечивающие информационную безопасность.

Анализ объекта данного преступления позволил автору констатировать несостоятельность и преждевременность встречающихся в отечественной доктрине уголовного права предложений о перемещении исследуемой статьи в главу, устанавливающую уголовную ответственность за преступления в сфере компьютерной информации.

В качестве предмета мошенничества в сфере компьютерной информации выступает имущество (вещи), в том числе безналичные и электронные деньги, а также бездокументарные ценные бумаги. К числу предметов компьютерного мошенничества следует также относить премиальные (дисконтные) денежные суррогаты, электронные финансовые активы, а равно информационные (электронные) объекты, приобретаемые лицами за реальные деньги и обладающие явно выраженной потребительской ценностью. Вместе с тем подобное представляется возможным только при условии применения аналогии и распространения на виртуальные объекты норм гражданского права о вещах и праве собственности.

По мнению автора, обман или злоупотребление доверием не являются обязательными (конструктивными) признаками состава мошенничества в сфере компьютерной информации, предусмотренного ст. 159.6 УК РФ. Способами совершения мошенничества в сфере компьютерной информации выступают: 1) ввод компьютерной информации; 2) удаление компьютерной информации; 3) блокирование компьютерной информации; 4) модификация компьютерной информации; 5) вмешательство в функционирование средств хранения компьютерной информации; 6) вмешательство в функционирование средств обработки компьютерной информации; 7) вмешательство в функционирование средств передачи компьютерной информации; 8) вмешательство в функционирование информационно-телекоммуникационной сети.

Определены признаки способа совершения мошенничества в сфере компьютерной информации: 1) действия совершаются в виртуальном пространстве посредством использования компьютерной информации; 2) манипуляции с компьютерной информацией могут быть сопряжены как с правомерным доступом к компьютерной информации (компьютерной системе), так и без такового; 3) действия не ориентированы на сознание человека (введение его в заблуждение); 4) манипуляции с компьютерной информацией направлены на изъятие чужого имущества (получение права на чужое имущество) и причинение имущественного ущерба потерпевшему.

Во втором параграфе «Субъективные признаки мошенничества в сфере компьютерной информации» автор исследует субъективные признаки мошенничества в сфере компьютерной информации автор делает вывод, что по смыслу ст. 159.6 УК РФ субъектом мошенничества в сфере компьютерной информации является физическое вменяемое лицо, достигшее на момент совершения деяния 16-летнего возраста (общий субъект). Им может быть как гражданин Российской Федерации, так и иностранный гражданин, а равно лицо без гражданства. Встречающееся в науке уголовного права предложение о необходимости понижении возраста уголовной ответственности, по мнению

соискателя, является преждевременным и требует комплексной проработки. Распространение уголовной ответственности на более широкий круг несовершеннолетних может повлечь негативные социальные последствия и вряд ли будет способствовать повышению эффективности борьбы с преступностью. Кроме того, законодательная обусловленность возраста привлечения к уголовной ответственности объясняется нераспространенностью подобного рода преступной деятельности среди лиц, не достигших 16-летнего возраста.

В работе обосновывается, что личность компьютерного мошенника может быть успешно представлена в рамках распространенного деления преступников на ситуационный и последовательно-криминогенный типы.

Для ситуационного типа свойственно совершение мошенничества вследствие сложившейся благоприятной ситуации, возникающей преимущественно по причине виктимного поведения самого потерпевшего.

Последовательно-криминогенный тип характеризуется устойчивой направленностью на совершение мошеннических действий в сфере компьютерной информации, ярко выраженной корыстной мотивацией (стремлением к накоплению значительных средств) и профессионализмом.

Субъективная сторона преступления, предусмотренного ст. 159.6 УК РФ, характеризуется умышленной формой вины в виде прямого умысла. Совершая мошенничество в сфере компьютерной информации, лицо осознает общественно опасный характер своих действий с использованием информационных технологий, предвидит неизбежность наступления общественно опасных последствий в форме незаконного обогащения за счет причинения имущественного ущерба потерпевшему и желает их наступления.

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

В третьем параграфе «Квалифицированные виды мошенничества в сфере компьютерной информации» автор отмечает, что установление признака значительного ущерба, крупного и особо крупного размера ущерба, причиненного в результате компьютерного мошенничества, может основываться на сложении сумм денежных средств в результате совершения лицом ряда тождественных действий по противоправному изъятию имущества.

Использование лицом возможностей, связанных с замещением должности и выполнением функций рядового работника (к примеру, системного администратора, специалиста по обслуживанию клиентов и продажам), не может служить основанием для квалификации содеянного по ч. 3 ст. 159.6 УК РФ как мошенничества в сфере компьютерной информации, совершенного лицом с использованием своего служебного положения.

По мнению диссертанта, при установлении признаков значительного ущерба, крупного и особо крупного размеров необходимо руководствоваться

общей стоимостью похищенного имущества (денежных средств) без учета ее фактического уменьшения в результате комиссионных сборов и удержаний банков, операторов платежных систем и др.

Наличие в ч. 4 ст. 159.6 УК РФ указания на организованную группу отвечает научно обоснованным критериям конструирования квалифицированных составов преступлений. Организованный характер группы при осуществлении компьютерного мошенничества, с одной стороны, значимо влияет на степень общественной опасности этого деяния, а с другой — не является характерным и не сопровождает большинство преступлений, предусмотренных ст. 159.6 УК РФ.

Полагая, что п. «в» ч. 3 ст. 159.6 УК РФ («с банковского счета, а равно в отношении электронных денежных средств»), введенный Федеральным законом от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации», противоречит научно обоснованным критериям дифференциации уголовной ответственности, автор предлагает исключить данное особо отягчающее обстоятельство из ст. 159.6.

Третья глава «Проблемы квалификации, совершенствования законодательства и предупреждения мошенничества в сфере компьютерной информации» состоит из трех параграфов.

Первый параграф «Проблемы квалификации мошенничества в сфере компьютерной информации» посвящен рассмотрению проблемных вопросов квалификации мошенничества в сфере компьютерной информации.

По мнению автора, единым продолжаемым преступлением следует признавать случаи совершения лицом компьютерного мошенничества способами, предполагающими автоматическое срабатывание вредоносного программного обеспечения, в результате которого происходит изъятие денежных средств потерпевших. При подобных обстоятельствах виновное лицо может не знать определенно, сколько граждан пострадает в результате его преступных действий, а также окончательный размер причиненного ущерба. Вместе с тем многочисленность совершенных трансакций, как и лиц, утративших имущество, не свидетельствует о совокупности преступлений.

Установлено, что лицо, склоняющее к совершению компьютерного мошенничества или оказывающее содействие неограниченному и не персонифицированному числу лиц, размещающее материалы с указанием «до востребования», имеет не абстрактное, а вполне конкретное намерение. Абстрактность самого исполнителя не меняет общего вывода о наличии причинной обусловленности и реальной взаимосвязи таких действий, то есть о наличии признаков соучастия.

По мнению диссертанта, методы нечестной электронной коммерции, рассчитанные на невнимательность потребителя, который не уделил должного внимания специальным условиям (как правило, едва заметным), указывающим на действительную стоимость продукта, не образуют признаков состава преступления, предусмотренного ст. 159.6 УК РФ.

Согласно ст. 159.6 УК РФ вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или

информационно-телекоммуникационных сетей признается целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные), снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него.

В связи с этим автор полагает ошибочным разъяснение Пленума Верховного Суда РФ о необходимости дополнительного вменения уголовно-правовой нормы о неправомерном доступе к компьютерной информации (ст. 272 УК РФ), изложенное в абз. 2 п. 20 постановления от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате».

Кроме того, автор аргументирует необходимость дополнения п. 21 названного постановления Пленума абзацем следующего содержания: «Когда хищение совершается путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным с последующим удалением, модификацией либо блокированием охраняемой законом компьютерной информации (например, лицо сначала по чужим данным заходит в личный кабинет клиента банка в сети «Интернет», осуществляет перевод денежных средств, и только потом меняет настройки доступа), содеянное требует дополнительной квалификации по статье 272 УК РФ».

Второй параграф «Совершенствование законодательства об ответственности за мошенничество в сфере компьютерной информации» посвящен рассмотрению основных направлений совершенствования законодательства об ответственности за мошенничество в сфере компьютерной информации и разработке конкретных предложений.

Встречающиеся в отечественной доктрине уголовного права предложения о полном исключении из УК РФ ст. 159.6 является принципиально неверным. Необходимость определения уголовной ответственности за совершение хищения путем использования компьютерной информации в рамках специальной нормы обусловлена, прежде всего, тем, что такие деяния при внешней схожести с традиционными формами хищения все же могут не подпадать ни под одну из них. И хотя название ст. 159.6 УК РФ действительно во многом имеет условный характер, деяние, описанное в ее диспозиции, нельзя путать с классическим мошенничеством. В ином случае это может привести к размыванию границ традиционного понимания мошенничества и может лишить его четкости и определенности.

Выделяя мошенничество в сфере компьютерной информации, законодатель прямо и недвусмысленно определил свое отношение к данной разновидности преступных деяний. Сравнительный анализ позволил автору сделать вывод, что данный состав преступления, по мысли законодателя, обладает разительно меньшей степенью общественной опасности в сравнении с общим составом

мошенничества. Изначально наиболее ярко это проявилось в дифференцированном подходе к определению крупного и особо крупного размеров ущерба. Совершение лицом компьютерного мошенничества в редакции до 23 апреля 2018 г. с ущербом свыше 1 млн руб., но в пределах 1 млн 500 тыс. руб., по ч. 2 ст. 159.6 УК РФ в качестве самого строгого наказания предполагало лишение свободы на срок до 4 лет. В то же время простое мошенничество за аналогичное деяние по ч. 4 ст. 159 УК РФ безальтернативно наказывается лишением свободы на срок до 10 лет.

Поскольку мошенники в сфере высоких технологий хорошо маскируют свою деятельность, что дает возможность совершать преступления длительное время и завладевать имуществом большого числа физических и юридических лиц, такое решение законодателя представлялось по меньшей мере дискуссионным.

Федеральный закон от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» исправил данный юридико-технический недостаток, определив крупный и особо крупный размеры мошенничества в сфере компьютерной информации в общем порядке в соответствии с примечанием 4 к ст. 158 УК РФ.

Проведенное автором социологическое исследование показало, что абсолютное большинство респондентов (в среднем 94 %) независимо от рода деятельности (судьи, следователи, оперативные работники, профессорско-преподавательский состав, представители коммерческих структур и др.) соглашаются с тем, что наказание за мошенничество в сфере компьютерной информации должно быть не мягче, чем за «классическое» мошенничество. При этом около 85 % респондентов поддерживают идею о необходимости закрепления более строгой санкции по сравнению с общей ст. 159 УК РФ.

Суммируя результаты проведенного социологического исследования, а также имеющиеся рекомендации в науке уголовного права, автор формулирует следующие положения:

- санкции, предусмотренные ст. 159.6 УК РФ, сконструированы без учета системно-структурных связей уголовно-правовых норм, при игнорировании понимания уголовного законодательства как целостной, внутренне непротиворечивой системы;

- санкции за совершение компьютерного мошенничества должны отражать усиление карательных функций государства и, следовательно, должны быть жестче санкций за кражу (ст. 158 УК РФ) или мошенничество (ст. 159 УК РФ).

С учетом приведенного предложена новая редакция ст. 159.6 УК РФ:

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

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

наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до трех лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до трех лет.

2. То же деяние, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину, а равно лицом, на которое по службе или работе возложены обязанности по обеспечению эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, либо с неправомерным доступом к охраняемой законом компьютерной информации, -

наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до пяти лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до одного года или без такового, либо лишением свободы на срок до пяти лет с ограничением свободы на срок до одного года или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные лицом с использованием своего служебного положения, а равно в крупном размере, -

наказываются штрафом 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, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового, либо лишением свободы на срок до семи 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.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, совершенные организованной группой либо в особо крупном размере, -

наказываются лишением свободы на срок до двенадцати 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».

В третьем параграфе «Проблемы предупреждения мошенничества в сфере компьютерной информации», рассматривая вопросы предупреждения мошенничества в сфере компьютерной информации, автор отмечает, что в системе криминогенных детерминант мошенничества в сфере компьютерной информации особую роль играет взаимодействие следующих факторов: а) низкий уровень культуры информационной безопасности населения; б) недостаточный объем финансирования программ по развитию систем защиты платежных операций;

в) просчеты в системе подбора и расстановки кадров кредитных организаций и компаний, оказывающих телематические услуги связи; г) ограниченные функциональные возможности отделов собственной безопасности кредитных организаций и их слабое взаимодействие с правоохранительными органами; д) несовершенство регулятивного законодательства в сфере трудовых отношений, информационной безопасности и электронной коммерции; е) низкая эффективность применения уголовно-правовых норм с двойной превенцией, а именно ст.ст. 272, 273, 274 и 274.1 УК РФ.

Не умаляя роли уголовного права в решении задачи предупреждения мошенничества в сфере компьютерной информации, автор отмечает, что построение эффективной превентивной стратегии кроется, главным образом, в принятии комплекса мер информационно-просветительского и технического характера.

По мнению диссертанта, в современных условиях предупреждение мошенничества в сфере компьютерной информации следует организовать на основе взаимодействия государственных органов, отраслевых структур и общественных организаций посредством проведения мониторинга информационных ресурсов на предмет обнаружения угроз, связанных с распространением сведений о неизвестных правоохранительным органам методах и способах компьютерного мошенничества, в целях дальнейшего блокирования данных ресурсов.

Разрабатываемый подход ограничения анонимности пользователей в сети «Интернет» должен пройти жесткую проверку с точки зрения концепции неприкосновенности частной жизни лица. Тотальный контроль за активностью в информационном пространстве не имеет принципиальных отличий от чипирования и слежки за человеком в реальном (физическом) мире. Таким образом автономия личности приносится в жертву соображениям необходимости обеспечения всеобщей информационной безопасности, что является недопустимым. Возможное решение должно быть сбалансированным и предполагать обязательную идентификацию лишь в строго ограниченных случаях (например, при регистрации в социальных сетях, размещении объявлений о продаже товаров и оказании услуг).

Действенное предупреждение мошенничества в сфере компьютерной информации возможно только в случае эффективного применения уголовно-правовых норм с двойной превенцией, а именно ст.ст. 272, 273, 274 и 274.1 УК РФ. Как представляется, для того чтобы они стали высокорезультативным средством противодействия киберпреступности, в том числе компьютерному мошенничеству, необходимо нейтрализовать факторы, снижающие их эффективность: отдельные просчеты и ошибки, допущенные при конструировании данных норм, избирательность их применения.

В значительной степени нереализованным превентивным зарядом предупреждения мошенничества в сфере компьютерной информации обладает положение п. 12 ст. 9 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе», согласно которому оператор по переводу

денежных средств обязан возместить клиенту сумму операции, совершенной без его согласия. Неукоснительное исполнение данной нормы позволит создать условия для формирования мотивации банковского сектора на ответственное отношение к вопросам безопасности и должное финансирование программ по развитию систем защиты платежных операций.

В **заключении** в краткой форме представлены основные научно-теоретические выводы и практические предложения по совершенствованию правоприменительной практики и уголовного законодательства.

По теме диссертации автором опубликованы следующие работы:

Статьи, опубликованные в изданиях, включенных в «Перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени доктора и кандидата наук»

1. *Фролов, М. Д.* Противодействие компьютерному мошенничеству в аспекте норм международного права // Вестник Владимирского юридического института. — 2015. — № 4 (37). — С. 124–128. — 0,3 п. л.

2. *Фролов, М. Д.* Уголовная ответственность за мошенничество в сфере компьютерной информации по законодательству стран Европы и СНГ // Учёные труды Российской академии адвокатуры и нотариата. — 2015. — № 4 (39). — С. 151–155. — 0,5 п. л.

3. *Фролов, М. Д.* Уголовная ответственность за мошенничество в сфере компьютерной информации по законодательству стран Северной и Южной Америки, Океании, Азии и Африки // Административное и муниципальное право. — 2015. — № 11. — С. 1164–1168. — 0,4 п. л.

4. *Фролов, М. Д.* О некоторых проблемах квалификации мошенничества в сфере компьютерной информации // Адвокат. — 2016. — № 6. — С. 53–58. — 0,5 п. л.

5. *Фролов, М. Д.* К вопросу об ответственности за мошенничество в сфере компьютерной информации // Образование и право. — 2018. — № 9. — 0, 4 п. л.

6. *Фролов, М. Д.* Предупреждение мошенничества в сфере компьютерной информации // Учёные труды Российской академии адвокатуры и нотариата. — 2018. — № 3 (50). — С. 86 –95. — 0,5 п. л.

В иных научных изданиях

7. *Фролов, М. Д.* К вопросу об объекте мошенничества в сфере компьютерной информации // Тенденции развития уголовного и уголовно-процессуального законодательства : материалы Международной научной конференции, посвященной 80-летию заслуженного юриста РФ, доктора юридических наук, профессора Махова Вадима Николаевича (Москва, 20 ноября 2015 г.) / отв. ред. Л. А. Букалерова. — М. : РУДН, 2016. — С. 491–498. — 0,3 п. л.

8. *Фролов, М. Д.* Предмет мошенничества в сфере компьютерной информации // Актуальные проблемы уголовного права и криминологии : материалы XI ежегодного межвузовского научно-практического круглого стола, посвященного Дню российской науки (Ставрополь, 19 февраля 2016 г.). / отв. ред. И. Г. Соломоненко. — Ставрополь, 2016. — С. 138–145. — 0,3 п. л.

9. *Фролов, М. Д.* Особенности мошенничества в сфере компьютерной информации, совершаемого лицом с использованием своего служебного положения // Научно-методическое обеспечение подготовки сотрудников органов внутренних дел в целях противодействия преступности : материалы

Всероссийского научно-методического семинара, посвященного 20-летию принятия Уголовного кодекса Российской Федерации (Руза, 13 мая 2016 г.) / под ред. д-ра юрид. наук, проф. Н. Г. Кадникова и д-ра юрид. наук, проф. И. М. Мацкевича. — М., 2017. — С. 206–210. — 0,4 п. л.

АННОТАЦИЯ

Фролов Михаил Дмитриевич

Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации

В диссертации проведен комплексный анализ норм отечественного, международного и зарубежного законодательства об ответственности за мошенничество в сфере информации и разработка научно обоснованных рекомендаций и предложений по преодолению проблем, возникающих в связи уголовно-правовым и криминологическим противодействием преступлениям в данной сфере.

Изучены международно-правовые стандарты и основные подходы к регламентации уголовной ответственности за мошенничество в сфере компьютерной информации, используемые в законодательстве зарубежных стран; определены социально-правовые основания криминализации мошенничества в сфере компьютерной информации; осуществлен юридический анализ состава преступления, предусмотренного ст. 159.6 УК РФ; выявлены недостатки уголовного законодательства об ответственности за совершение преступления, предусмотренного ст. 159.6 УК РФ; сформулированы предложения по совершенствованию конструкции состава преступления, предусмотренного ст. 159.6 УК РФ и разработаны предложения по предупреждению мошенничества в сфере компьютерной информации.

Frolov Mikhail Dmitrievich

Criminal law and criminological counteraction of cybercrime

In the thesis a comprehensive analysis of domestic, international and foreign legislationnorms on liability for cyber fraud was conducted and scientifically based recommendations and proposals on overcoming problems arising in connection with criminal law and criminological counteraction of cyber-crime were developed.

International legal standards and basic approaches to the regulation of cyber-crime criminal liability used in the legislation of foreign countries were studied; social and legal grounds for criminalization of cyber fraud were determined; a legal analysis of the corpus delicti provided for under art. 159.6 of the Russian Fed. Criminal Code was conducted; the shortcomings of criminal legislation on liability for committing a crime under Art. 159.6 of the Criminal Code were revealed; proposals for improving the construction of the criminal action under Art. 159.6 of the Criminal Code of the Russian Federation were formulated and proposals for cybercrime prevention were developed.