

*На правах рукописи*

**Григорян Гарик Рафикович**

**МОШЕННИЧЕСТВО В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ:  
ПРОБЛЕМЫ КРИМИНАЛИЗАЦИИ, ЗАКОНОДАТЕЛЬНОЙ  
РЕГЛАМЕНТАЦИИ И КВАЛИФИКАЦИИ**

12.00.08 – Уголовное право и криминология; уголовно-исполнительное право

Автореферат диссертации на соискание ученой степени кандидата  
юридических наук

Самара – 2021

Работа выполнена в федеральном государственном автономном образовательном учреждении высшего образования «Самарский национальный исследовательский университет имени академика С.П. Королева» на кафедре уголовного права и криминологии

Научный руководитель:

доктор юридических наук, профессор **Безверхов Артур Геннадьевич**

Официальные оппоненты:

**Ефремова Марина Александровна**, доктор юридических наук, доцент, Казанский филиал федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный университет правосудия», кафедра уголовно-правовых дисциплин, профессор

**Серебrenникова Анна Валерьевна**, доктор юридических наук, доцент, федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный университет имени М.В. Ломоносова», кафедра уголовного права и криминологии, профессор

**Ведущая организация:** федеральное государственное бюджетное образовательное учреждение высшего образования «Кубанский государственный аграрный университет имени И.Т. Трубилина», г. Краснодар

Защита состоится 19 июня 2021 г. в 10.00 час. на заседании диссертационного совета Д 212.215.09 на базе федерального государственного автономного образовательного учреждения высшего образования «Самарский национальный исследовательский университет имени академика С. П. Королева» по адресу: г. Самара, ул. Академика Павлова, 1, Самарский университет, корпус 22-в, зал заседаний.

С диссертацией можно ознакомиться в библиотеке и на сайте федерального государственного автономного образовательного учреждения высшего образования «Самарский национальный исследовательский университет имени академика С. П. Королева» [https://ssau.ru/resources/dis\\_protection/grigoryan](https://ssau.ru/resources/dis_protection/grigoryan).

Автореферат разослан « \_\_\_\_ » \_\_\_\_\_ 2021 г.

Ученый секретарь  
диссертационного совета Д 212.215.09

Норвартян Ю.С.

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность темы диссертационного исследования.** Современный этап развития Российской Федерации характеризуется масштабными трансформациями в сфере цифровой экономики и в других областях социальной жизнедеятельности, где главными богатствами и силой становятся данные, сообщения, знания, информация, в том числе компьютерная информация. Политико-правовые основы цифровизации в России заложены в стратегических программных документах: Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы, утвержденная Указом Президента Российской Федерации от 9 мая 2017 г. № 203; Указ Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»; Перечень поручений по вопросам реализации национальной программы «Цифровая экономика Российской Федерации», утвержденный Президентом Российской Федерации 28 февраля 2019 г. № Пр-300; Паспорт национального проекта «Национальная программа "Цифровая экономика Российской Федерации"» (утв. Президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам, протокол от 4 июня 2019 г. № 7); государственная программа Российской Федерации «Информационное общество», утвержденная постановлением Правительства Российской Федерации от 15 апреля 2012 № 313 (ред. от 16 декабря 2020 г.) и др.

Реализация стратегии перехода к цифровой экономике обеспечивается всеми отраслями российского права, среди которых немаловажную роль продолжает играть уголовное право, призванное гарантировать надежную правовую охрану новым базисным отношениям, характерным для постиндустриального общества, в целях обеспечения качества жизни граждан, экономического роста и национального суверенитета. Федеральным законом от 29 ноября 2012 г. № 207-ФЗ в Уголовный кодекс Российской Федерации (далее – УК РФ) введена статья 159<sup>6</sup> «Мошенничество в сфере компьютерной информации», которая получила неоднозначную оценку в науке уголовного права и криминологии. Критически восприняты также Федеральные законы от 3 июля 2016 г. № 325-ФЗ и от 23 апреля 2018 г. № 111-ФЗ, которыми были внесены изменения в ст. 159<sup>6</sup> УК РФ. Противоречивая практика применения положений, предусмотренных ст. 159<sup>6</sup> и смежными статьями УК РФ об ответственности за имущественные и иные преступления в сфере компьютерной информации (п. «г» ч. 3 ст. 158, ст. 159<sup>3</sup>, ст. 272-274<sup>1</sup>), подтверждает запрос на научное обоснование совершенствования содержания соответствующих уголовно-правовых норм и опыта их реализации.

Цифровая реальность предоставляет человечеству невероятные возможности, одновременно порождая большие вызовы и глобальные проблемы. Одна из них – стремительный рост преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, в том

числе преступлений против собственности в сфере компьютерной информации. Эти преступления выражаются в совершении различных корыстных имущественных действий в сфере информационно-телекоммуникационных сетей с использованием компьютерной информации и электронных (цифровых) технологий. Как отметил Президент Российской Федерации В.В. Путин на ежегодном расширенном заседании коллегии Министерства внутренних дел Российской Федерации, состоявшемся 3 марта 2021 г., за последние 6 лет число преступлений в сфере информационных технологий возросло более чем в 10 раз. Наша задача – эффективно ответить на этот криминальный вызов, защитить граждан и добросовестный бизнес, который активно осваивает цифровое пространство.

Преступления, совершенные с использованием IT-технологий, составляют всё большую долю в общей структуре преступности: сегодня она достигла 25 процентов. В последние несколько лет фиксируется динамика ежегодного прироста таких деликтов. Так, в 2019 г. зарегистрировано более 294 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий, что на 70 % больше, чем за 2018 г. Половина таких преступлений совершается с использованием сети «Интернет», а более трети – посредством мобильной связи. В 2020 г. зарегистрировано 510,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий, что на 73,4 % больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 14,5 % в 2019 г. до 25,0 % в 2020 г. Больше половины (58,8 %) таких преступлений совершается с использованием сети «Интернет» (300,3 тыс. (+91,3 %)), почти половина (42,9 %) – с использованием средств мобильной связи (218,7 тыс. (+88,3 %)). Четыре таких преступления из пяти (80,4%) совершаются путем кражи или мошенничества (410,5 тыс. (+74,3 %)). По итогам первых двух месяцев 2021 г. общее число зарегистрированных в стране тяжких и особо тяжких преступлений возросло на 2,8 %. Основной причиной этого является увеличение количества криминальных деяний данной категории, совершенных с использованием информационно-телекоммуникационных технологий. За два месяца текущего года в Российской Федерации зарегистрировано на 29,4 % больше IT-преступлений, чем год назад, в том числе совершенных с использованием сети «Интернет» – на 48,3 % и при помощи средств мобильной связи – на 32,6 %. Если в январе-феврале 2020 г. удельный вес преступлений в IT-сфере составлял 19,3 %, то за первые 2 месяца 2021 г. он увеличился до 26,3 %.

Количество преступлений, совершенных в форме мошенничества (ст. 159-159<sup>6</sup> УК РФ), за 2019 г. по сравнению с 2018 г. увеличилось на 19,6 % и составило 257 187 преступлений. В результате в структуре преступности их доля увеличилась с 12,7 % до 16,4 %. Наиболее распространено мошенничество в сфере информационно-телекоммуникационных технологий или компьютерной информации, на них приходится около 70 % всех хищений, совершенных путем обмана или злоупотребления доверием (+73,4 %, 237,1

тыс.). При совершении 25,8 тыс. (+42,4 %) мошенничеств использовались электронные средства платежа. При этом следует подчеркнуть, что мошенничество и иные преступления в сфере компьютерной информации в силу их полиномической природы и скрытого характера отличаются высокой латентностью.

В современной теории, законодотворчестве и правоприменении становятся все более выраженными проблемы криминализации, законодательной регламентации и квалификации «мошенничества в сфере компьютерной информации», «мошенничества с использованием электронных средств платежа» и «кражи, совершенной с банковского счета, а равно в отношении электронных денежных средств». Речь идет о своеобразной «триаде», сконструированной законодателем в целях восполнения пробелов УК РФ для обеспечения уголовно-правовой охраны новых экономических отношений путем расширения сферы действия «традиционных» норм о хищении чужого имущества и приобретении права на чужое имущество. Рассредоточение положений об имущественных преступлениях в сфере информационно-телекоммуникационных технологий по разным статьям главы 21 УК РФ, а также использование нормативных предписаний о краже и мошенничестве как аналогий закона в целях противодействия «цифровым» имущественным преступлениям – сравнительно новым общественно опасным посягательствам, находятся в противоречии с единой социально-правовой сущностью и своебытной характеристикой соответствующих преступных деяний, не учитывают особенности их объекта (в том числе предмета), характера и содержания действий, способа и средства совершения преступного деяния, момента окончания преступления и др.

Становление постиндустриального общества и цифровой экономики требует переосмысления парадигмы уголовно-правовой охраны сложных (комплексных) общественных отношений, в том числе складывающихся на стыке двух сфер – информационной и экономической. При этом новые (включая виртуальные) реальности с ускоряющимися процессами разработки и внедрения высоких технологий определяют необходимость формирования и применения в законодательной и правоприменительной практиках принципиально нестандартных подходов, позиций и решений в соответствующих областях уголовно-правового противодействия.

Обращают на себя внимание недостатки юридической техники, касающиеся таких положений главы 21 УК РФ, как «хищение чужого имущества путем ввода, удаления, блокирования, модификации компьютерной информации», «приобретение права на чужое имущество путем вмешательства в функционирование информационно-телекоммуникационных сетей», «хищение чужого имущества с банковского счета», «кража, совершенная в отношении электронных денежных средств», «изъятие денежных средств с расчетного счета их владельца» и др. Как показано в настоящей диссертации, они вызваны необоснованным использованием юридических средств, правил и приемов разработки конструкций вещных преступлений против собственности

для противодействия ранее не известным имущественным преступлениям в сфере компьютерной («цифровой», «электронной») информации. Когда в область современной уголовно-правовой материи вторгаются новые криминальные явления, а действующие законодательные конструкции (даже при их модернизации) не позволяют эффективно решать проблемы правовой охраны формирующихся базисных отношений, появляется потребность в создании таких уголовно-правовых новелл, которые способны эффективно регулировать образующийся сегодня общественно-экономический уклад в целях надежного обеспечения цифровой безопасности России.

Необходимость научного анализа обозначенной проблематики предопределяется также поиском путей оптимизации практики применения уголовно-правовых норм об ответственности за указанные посягательства и смежные с ними преступления.

**Степень научной разработанности темы исследования.** Новизна рассматриваемой проблематики обусловлена недостаточной исследованностью в науке темы настоящей диссертации. Вместе с тем отдельные вопросы криминализации, пенализации, законодательной регламентации и квалификации мошенничества в сфере компьютерной информации и смежных с ним преступлений нашли отражение в трудах И.А. Александровой, И.Р. Бегишева, А.Г. Безверхова, Л.М. Болсуновской, Л.А. Букалеровой, А.Б. Волеводз, А.В. Гладких, М.Ю. Дворецкого, К.Н. Евдокимова, В.М. Елина, О.В. Ермаковой, М.А. Ефремовой, А.С. Камко, Н.Ш. Козаева, А.А. Комарова, Т.А. Кули-Заде, Н.А. Лопашенко, С.С. Медведева, И.А. Мусьял, В.Ю. Окружко, М.А. Простосердова, Е.А. Русскевича, О.М. Сафонова, А.В. Серебренниковой, Е.А. Соловьевой, М.И. Третьяк, В.И. Тюнина, М.Д. Фролова, З.И. Хисамова, В.В. Челнокова, А.Ю. Чупровой, А.В. Шульги, А.А. Южина, П.С. Яни и др.

Отдельным аспектам исследуемой проблематики посвящены докторские диссертации М.А. Ефремовой «Уголовно-правовая охрана информационной безопасности» (2018 г.) и Н.Ш. Козаева «Современные проблемы уголовного права, обусловленные научно-техническим прогрессом» (2016 г.), а также кандидатские диссертации М.А. Простосердова «Экономические преступления, совершаемые в киберпространстве, и меры противодействия им» (2016 г.), А.А. Южина «Мошенничество и его виды в российском уголовном праве» (2016 г.), И.А. Мусьял «Дифференцированные виды мошенничества: теоретические и практические проблемы» (2018 г.), М.Д. Фролова «Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации» (2018 г.).

**Объектом диссертационного исследования** являются общественные отношения, возникающие в связи с совершением мошенничества в сфере компьютерной информации и смежных с ним преступлений.

**Предмет диссертационного исследования** образуют нормы современного российского и зарубежного уголовного законодательства об ответственности за мошенничество и смежные с ним преступления в сфере компьютерной информации, а также отдельные нормативно-правовые положения

действующего законодательства России по обеспечению безопасности, об информации, информационных технологиях и защите информации, объектах гражданских прав, национальной платежной системе, цифровых финансовых активах, цифровой валюте и др.; практика применения уголовно-правовых норм о мошенничестве в сфере компьютерной информации и смежных с ним преступлений; доктринальные разработки вопросов уголовной ответственности за экономические и иные преступления в сфере компьютерной информации.

**Цель диссертационного исследования** состоит в обосновании концептуального подхода к пониманию «компьютерного» мошенничества как самостоятельной разновидности преступлений против собственности, совершаемых в сфере компьютерной информации, и разработке в рамках этого подхода научно обоснованных рекомендаций по совершенствованию уголовного законодательства России об ответственности за имущественные преступления в сфере использования компьютерной информации и техники, а также практики его применения в условиях становления и развития постиндустриального общества и цифровой экономики.

Достижение поставленной цели определяет решение следующих **задач**:

- философско-социологическое осмысление причин криминализации «компьютерного» мошенничества и его социально-правовой природы; исследование информационно-технологических, социально-экономических и криминологических оснований уголовно-правового запрета мошенничества и иных имущественных преступлений в сфере компьютерной информации;
- изучение опыта отдельных стран ближнего и дальнего зарубежья в части регламентации уголовной ответственности за мошенничество и иные имущественные преступления в сфере компьютерной информации;
- определение понятия, видов и значения объекта мошенничества в сфере компьютерной информации;
- выявление особенностей объективной стороны мошенничества в сфере компьютерной информации;
- юридико-технический анализ субъективных признаков мошенничества в сфере компьютерной информации;
- рассмотрение вопросов дифференциации уголовной ответственности за преступления, предусмотренные статьей 159<sup>б</sup> Уголовного кодекса Российской Федерации;
- разработка и обоснование предложений по совершенствованию отдельных положений уголовного законодательства России об ответственности за имущественные преступления в сфере компьютерной информации и практики его применения.

**Научная новизна диссертационного исследования** состоит в том, что оно является первым специальным комплексным теоретико-прикладным исследованием, посвященным вопросам криминализации, законодательной регламентации и квалификации мошенничества в сфере компьютерной информации. В диссертации освещаются ранее не изученные или малоисследованные вопросы об основаниях и пределах криминализации

нарушений имущественных прав и интересов в сфере информационно-телекоммуникационных технологий и компьютерной информации, об особенностях социально-правовой природы «цифровых» преступлений против собственности. Новизна настоящей диссертации состоит также в разработке авторской модели уголовно-правовой нормы об ответственности за умышленное причинение имущественного ущерба путем неправомерного воздействия на объекты в сфере информационно-телекоммуникационной сети и компьютерной информации и рекомендаций по отдельным вопросам судебной практики по делам об имущественных и смежных с ними преступлениях в сфере компьютерной информации. На основании сделанных выводов внесены предложения по оптимизации действующего уголовного законодательства.

**Теоретическая и практическая значимость диссертации** связана с решением научных, законотворческих и правоприменительных задач. Теоретическое значение исследования состоит в том, что его результаты дополняют и развивают современное учение об умышленных преступлениях против собственности. В диссертации уточнены социально-правовая сущность отдельных посягательств на собственность и характеристики понятийно-категориального аппарата, предусмотренного главой 21 УК РФ. Сформулированные в работе выводы и рекомендации могут быть использованы в ходе дальнейших научных исследований, посвященных проблемам криминализации и пенализации общественно опасных нарушений имущественных прав и интересов в сфере цифровой экономики, а также составить научные основы систематизации уголовного законодательства России о преступлениях против собственности, законодательной регламентации и квалификации имущественных преступлений, совершаемых в сфере компьютерной информации.

Практическая значимость диссертации заключается в возможности применения ее положений и выводов при определении современной уголовной политики в сфере цифровой экономики, в законотворческой деятельности и правоприменительной практике.

Результаты исследования могут найти применение в преподавании курсов «Уголовное право», «Криминология», «Уголовная политика», «Преступления против собственности», «Цифровое право», «Юридическая техника», а также в системе повышения квалификации работников суда, прокуратуры, следствия, адвокатуры.

**Методология и методы диссертационного исследования.** Методология обусловлена целями и задачами исследования. Методологическую основу диссертации составляют философско-социологическое и информационно-философское познание права, общенаучное исследование права и юридико-догматическое (в том числе междисциплинарное) освоение права.

В исследовании использованы диалектический метод, информационный и кибернетический подходы, общенаучные методы дедукции, индукции и интерпретации, анализа и синтеза, аналогии, частнонаучные методы познания:

системно-структурный, социологический, формально-логический, сравнительно-правовой, юридико-технический и другие.

**Теоретическую основу диссертационного исследования** составили труды по философии, социологии, информатике, криптологии, теории государства и права, конституционному, административному, гражданскому и другим отраслям юридического знания, а также научные труды российских ученых-юристов в области противодействия преступлениям против собственности (в том числе совершаемым в сфере цифровой экономики и компьютерной информации) и смежным с ними преступлениям: О.А. Адоевской, И.А. Александровой, И.Р. Бегишева, А.Г. Безверхова, В.В. Блажеева, Л.М. Болсуновской, Л.А. Букалеровой, А.Б. Волеводз, Р.Р. Галиакбарова, А.В. Гладких, Ю.В. Грачевой, М.Ю. Дворецкого, К.Н. Евдокимова, В.М. Елина, О.В. Ермаковой, М.А. Ефремовой, А.С. Камко, Т.В. Кленовой, Н.Ш. Козаева, А.А. Комарова, А.И. Коробеева, Л.Л. Кругликова, В.Н. Кудрявцева, Т.А. Кули-Заде, Н.А. Лопашенко, С.С. Медведева, И.А. Мусьял, А.В. Наумова, Ю.С. Норвартяна, В.Ю. Окружко, М.А. Простосердова, А.И. Розенцвайг, Е.А. Русскевич, О.М. Сафонова, А.В. Серебренниковой, Е.А. Соловьевой, М.И. Третьяк, В.И. Тюнина, М.Д. Фролова, Т.Я. Хабриевой, З.И. Хисамова, В.В. Челнокова, А.Ю. Чупровой, А.И. Чучаева, А.В. Шульги, А.А. Южина, П.С. Яни и других ученых-юристов.

Для целей исследования информационно-технологических и социально-экономических оснований криминализации нарушений имущественных прав и интересов в сфере компьютерной информации изучены труды Д. Белла, О.О. Варламова, Н. Винера, Л.С. Воскова, М. Кастельса, П.Л. Машенко, М.О. Пилипенко, Э. Тоффлера, Х. Тоффлера, Д. Уилера, С. Хокинга, А.А. Чернова, К. Шеннона и других ученых.

**Нормативная база** представлена положениями Конституции Российской Федерации, международного права, уголовного законодательства России и зарубежных стран, действующего гражданского законодательства и иных нормативных правовых актов, регулирующих порядок оказания платежных услуг, в том числе осуществления перевода денежных средств, использования электронных средств платежа, а также отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, применение информационных технологий, обеспечение защиты информации.

**Эмпирическую основу исследования** составили статистические данные ГИАЦ МВД о состоянии преступности в Российской Федерации и Самарской области за период 2012–2020 гг., решения судов общей юрисдикции России по имущественным преступлениям в сфере компьютерной информации за 2013–2021 гг., материалы 162 уголовных дел о мошенничестве в сфере компьютерной информации и смежных преступлениях; результаты анкетирования и интервьюирования 135 юристов, среди которых преподаватели юридических факультетов и вузов, сотрудники следственных органов, судьи, прокурорские и адвокатские работники.

### **На защиту выносятся следующие положения:**

1. Развитие информатизации и цифровых технологий предопределило кардинальные изменения в современном обществе, негативные последствия которых связаны с появлением и ростом новой разновидности преступлений против собственности, совершаемых в сфере компьютерной информации, информационно-телекоммуникационных сетей и технологий. Однако новые криминальные вызовы в сфере складывающихся базисных отношений, основанных на использовании компьютерной информации и цифровых технологий, опережают их уголовно-правовое регулирование. Ускоренное распространение высоких технологий в российском обществе, а также негативное влияние цифровых и электронных средств на формирование криминологического статуса современного социума требуют динамичного и поступательного развития отечественного уголовного законодательства в сфере компьютерной информации. При этом преступления, посягающие на новые общественные отношения, связанные со становлением и развитием информационного общества и цифровой экономики, а также совершаемые с применением высоких технологий (посредством компьютерной информации, технических и программных (электронных) средств и устройств, с использованием информационно-телекоммуникационной сети, в том числе сети «Интернет»), обладают повышенной общественной опасностью.

2. В условиях становления и развития информационного общества и цифровой экономики, а также особой криминологической обстановки, связанной с распространением в современном обществе ранее неизвестной разновидности имущественной преступности в сфере компьютерной информации, необходимо переосмысление парадигмы уголовно-правовой охраны традиционных отношений собственности с равномерным смещением акцентов в сторону защиты имущественных отношений неимущественного (нефизического) содержания от различного рода неправомерных нарушений и злоупотреблений, совершаемых в сфере высоких технологий.

При этом разработка новых концептуальных подходов к криминализации, пенализации и законодательной регламентации общественно опасных форм воздействия на набирающую силу цифровую трансформацию современного общества и его экономики должна обеспечить надежную охрану активно развивающихся «электронных» и «цифровых» форм имущественных отношений от всякого рода корыстных нарушений и злоупотреблений, совершаемых с применением информационно-телекоммуникационных технологий.

3. В процессе криминализации корыстных нарушений имущественных прав и интересов в киберпространстве следует учитывать, что:

- информационно-технологические факторы обусловленности уголовно-правовой охраны имущественных отношений детерминированы становлением информационного общества;

- факторы социально-экономической обусловленности уголовно-правовой охраны имущественных отношений связаны с развитием цифровой экономики.

4. Особенность преступлений, предусмотренных ст. 159<sup>б</sup> УК РФ, состоит в множественности объектов, неразрывно связанных с социально-экономическими, информационно-технологическими и другими общественными отношениями. Преступления против собственности, совершаемые в сфере компьютерной информации, могут причинять или угрожать причинением имущественного и иных видов вреда. Одним из дополнительных объектов преступлений, предусмотренных ст. 159<sup>б</sup> УК РФ, является информационная безопасность.

5. Предметом преступлений, предусмотренных ст. 159<sup>б</sup> УК РФ, выступает незаконная имущественная выгода в виде наличных или безналичных денег, электронных денежных средств, иного имущества, в том числе цифровых и иных имущественных прав.

6. Особенностью объективной стороны преступлений, предусмотренных ст. 159<sup>б</sup> УК РФ, выступают способ и средства совершения криминального посягательства, характеризующиеся несанкционированным воздействием на компьютерную информацию, неправомерным использованием компьютерных информационных технологий и технических средств, в том числе средств вычислительной техники, а равно вмешательством в функционирование электронных технических средств, их систем или информационно-телекоммуникационной сети.

7. Способом преступлений, описанных в ст. 159<sup>б</sup> УК РФ, является неправомерное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационной сети, в результате которого система обработки данных совершает информационно-вычислительные операции, сопряженные с передачей имущества или уступки имущественного права другому лицу либо совершения иного действия имущественного характера.

Формами неправомерного вмешательства являются ввод, удаление, блокирование, модификация, иное неправомерное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационной сети.

«Тайность», «открытость», «обман», «злоупотребление доверием», «удержание», «распоряжение» чужим имуществом и другие традиционные способы преступного посягательства на имущественные отношения отступают на задний план с развитием информационно-технологических форм передачи, получения, обработки электронных данных, сообщений с помощью средств вычислительной техники, системы ЭВМ, информационно-телекоммуникационной сети и сети ЭВМ.

8. Средством совершения преступлений, ответственность за которые установлена ст. 159<sup>б</sup> УК РФ, является «триада» технических и электронных средств в виде (1) компьютерной информации, (2) средств хранения, обработки или передачи компьютерной информации (средств вычислительной техники, электронных вычислительных машин и/или систем электронных вычислительных машин) и (3) информационно-телекоммуникационной сети.

Средства совместно со способом совершения предусмотренных ст. 159<sup>б</sup> УК РФ преступлений указывают на один из дополнительных объектов рассматриваемого преступного посягательства – информационную безопасность.

9. Механизм уголовно-правовой охраны имущественных отношений нуждается в конструировании новых составов преступлений, смежных с «традиционными» мошенничеством (совершаемым с использованием обмана или злоупотребления доверием) и хищением чужого имущества (совершаемым в отношении исключительно чужих вещей как объектов физического, материального мира). Он призван при этом обеспечить эффективное противодействие как реальным, так и потенциальным криминальным угрозам в складывающейся и развивающейся цифровой реальности.

10. В целях эффективного уголовно-правового противодействия преступлениям против собственности в сфере компьютерной информации представляется целесообразным дополнить УК РФ новой статьей 165<sup>1</sup> «Причинение имущественного ущерба путем неправомерного воздействия на объекты в сфере информационно-телекоммуникационной сети и компьютерной информации». Предметом этого преступления целесообразно признать любую незаконную имущественную выгоду в виде наличных или безналичных денег, электронных денежных средств, иного имущества, в том числе цифровых и иных имущественных прав, выполнения работ или оказания услуг имущественного характера, а равно иного необоснованного полного или частичного освобождения от имущественных обязательств, а равно неправомерного извлечения каких-либо других материальных привилегий или преимуществ. Также следует поставить вопрос о возможном отнесении криптовалюты и цифровой валюты к предмету преступлений, предусмотренных ст. 165<sup>1</sup> УК РФ.

Дополнение уголовного закона в близком или отдаленном будущем новыми составами имущественных нарушений с использованием информационно-телекоммуникационных технологий потребует исключения из УК РФ группы взаимосвязанных положений, содержащихся в п. «г» ч. 3 ст. 158 об ответственности за кражу, совершенную с банковского счета, а равно в отношении электронных денежных средств, в ст. 159<sup>б</sup> о мошенничестве с использованием электронных средств платежа и ст. 159<sup>а</sup> о мошенничестве в сфере компьютерной информации.

11. Сформулированы и мотивированы предложения о внесении 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».

**Степень достоверности результатов исследования.** Достоверность выводов и результатов, представленных в настоящей диссертации, обусловлена научной методологией исследования, использованием репрезентативной совокупности социологических и статистических данных, обширной теоретической базой в виде положений и выводов, содержащихся в

фундаментальных и прикладных научных трудах отечественных и зарубежных ученых, а также апробацией результатов диссертационного исследования на научных и научно-практических конференциях различного уровня.

**Апробация результатов исследования.** Теоретические и практические выводы по теме диссертации нашли отражение в девяти научных статьях, шесть из которых опубликованы в рецензируемых научных журналах, перечень которых установлен Министерством науки и высшего образования Российской Федерации.

Результаты исследования обсуждались на научных конференциях, среди которых: научно-практическая конференция «Правосудие по экономическим спорам: актуальные проблемы теории и практики (к 25-летию принятия Концепции судебной реформы в России)» (21-22 сентября 2016 г., г. Самара); международная научно-практическая конференция «Право, информационное общество и технологии» (16 ноября 2017 г., г. Самара); XV международная научно-практическая конференция «Уголовное право: стратегия развития в XXI веке» (25-26 января 2018 г., МГЮА, г. Москва); XI Российский конгресс уголовного права «Обеспечение национальной безопасности – приоритетное направление уголовно-правовой, криминологической и уголовно-исполнительной политики» (31 мая – 1 июня 2018 г., МГУ имени М.В. Ломоносова, г. Москва); XVI международная научно-практическая конференция «Уголовное право: стратегия развития в XXI веке» (24-25 января 2019 г., МГЮА, г. Москва); XVII международная научно-практическая конференция «Уголовное право: стратегия развития в XXI веке» (23-24 января 2020 г., МГЮА, г. Москва); XII Российский конгресс уголовного права «Эффективность уголовно-правового, криминологического и уголовно-исполнительного противодействия преступности» (28-29 мая 2020 г., МГУ имени М.В. Ломоносова, г. Москва); международный правовой банковский форум (24-25 сентября 2020 г., г. Самара). Соискатель принимал участие в круглом столе «Мошенничество в сфере компьютерной информации: вопросы квалификации» (15 февраля 2021 г., Клуб уголовного права «De lege lata» и Научно-образовательный центр «Уголовно-правовая экспертиза» юридического факультета МГУ имени М.В. Ломоносова, г. Москва) и круглом столе «Квалификация преступлений: общие и частные проблемы» (24 февраля 2021 г., Университет прокуратуры Российской Федерации, Клуб уголовного права «De lege lata» и Научно-образовательный центр «Уголовно-правовая экспертиза» юридического факультета МГУ имени М.В. Ломоносова, г. Москва). Соискатель является лауреатом Самарского областного конкурса «Молодой ученый» за научно-исследовательскую работу «Мошенничество в сфере компьютерной информации» в номинациях «Студент» (2017 г.) и «Аспирант» (2019 г.).

**Работа состоит** из введения, трех глав, включающих девять параграфов, заключения, списка литературы.

## ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы диссертационного исследования, определяются степень ее научной разработанности, объект и предмет, цель и задачи исследования, характеризуется теоретическая и практическая значимость диссертации, ее научная новизна, раскрываются теоретические основы и эмпирическая база исследования, излагаются основные положения, выносимые на защиту, приводятся обоснования достоверности и сведения об апробации результатов исследования и др.

**Первая глава** *«Мошенничество в сфере компьютерной информации: социально-правовой и юридико-компаративистский анализ»* включает три параграфа, в которых раскрываются социально-экономические, информационно-технологические и криминологические основания уголовно-правового запрета мошенничества в сфере компьютерной информации и проводится его сравнительно-правовое исследование с привлечением уголовного законодательства некоторых зарубежных стран.

**В первом параграфе** *«Социально-экономические и информационно-технологические основания криминализации мошенничества в сфере компьютерной информации»* утверждается, что философско-социологическое осмысление причин криминализации «компьютерного» мошенничества и его социально-правовой природы основывается на положениях теории информации как нематериальной сущности, а также концепций постиндустриального (информационного) общества и цифровой экономики. При этом информационно-технологические факторы обусловленности уголовно-правовой охраны экономических отношений тесно связаны с процессами формирования информационного общества. Переходя к вопросу о социально-экономических предпосылках уголовно-правовой охраны имущественных отношений, облакаемых в новые информационно-технологические формы, прежде всего укажем на процесс становления в современной России цифровой экономики. Темпы развития общественных отношений, основанных на использовании новых цифровых технологий, в том числе на технологии блокчейн, опережают правовое регулирование и охрану, что обуславливает необходимость ускорения законодательного реагирования на формирование и развитие нового комплекса производственных отношений с установлением четких границ и объема его правового регулирования и охраны.

В контексте социальных оснований криминализации установлено, что мошенничество в сфере компьютерной информации («компьютерное» мошенничество) – это сравнительно новый и малоисследованный тип преступного поведения, возникший в условиях цифровизации современного социума и совершаемый с использованием компьютерной информации, средств электронной вычислительной техники и информационно-телекоммуникационных сетей. Такой тип криминальной активности находит свое проявление на фоне формирования постиндустриальной цивилизации, информационного общества и цифровой экономики. «Компьютерное»

мошенничество нельзя сводить к хищению чужого имущества и к неправомерному приобретению права на чужое имущество.

Социальная обусловленность уголовно-правовых норм о «компьютерном» мошенничестве и сходных с ним корыстных имущественных преступлениях состоит в попытках законодателя обеспечить охрану складывающихся электронных, цифровых имущественных отношений от корыстных нарушений и злоупотреблений, совершаемых в сфере компьютерной информации с применением информационно-телекоммуникационных технологий. Здесь российское уголовное законодательство делает только первые шаги, пытаясь объективно отразить в положениях Особенной части УК РФ криминальную реальность, тесно связанную с виртуальным пространством общественной жизни, и защитить активно развивающиеся «электронные» и «цифровые» формы имущественных отношений.

Соискатель полагает, что по мере развития информационного общества и цифровых технологий составы преступлений, предусмотренных в ст. 159<sup>3</sup> и 159<sup>6</sup> УК РФ и относящихся к числу специальных видов мошенничества, будут трансформироваться в самостоятельные виды имущественных преступлений или даже отдельную группу корыстных преступных посягательств, совершаемых во взаимосвязанных сферах имущественных и информационно-технологических отношений.

**Во втором параграфе** *«Криминологические основания уголовно-правового запрета мошенничества в сфере компьютерной информации»* указывается, что развитие информатизации и цифровых технологий предопределило кардинальные изменения в рыночной экономике, негативные последствия которых связаны с появлением и ростом новых имущественных преступлений, совершаемых с использованием компьютерной информации, информационно-телекоммуникационных технологий, связанных с безналичными расчетами, платежными системами, технологией блокчейн, электронными торговыми площадками, электронными деньгами, цифровой валютой и т.д.

В параграфе на основе статистических данных и диаграмм иллюстрируется устойчивый рост мошенничеств и преступлений с использованием информационно-телекоммуникационных технологий. При этом обращается внимание на гиперлатентность мошенничества и его специальных видов, а также смежных с ним преступлений в сфере экономики. Прогнозируется дальнейший рост числа таких преступлений, которые будут модифицировать и усложнять свои формы с развитием постиндустриализма и цифровой экономики.

Соискателем утверждается, что имущественные преступления, посягающие на новые общественные отношения с помощью высокотехнологичных средств и с использованием современной компьютерной техники, характеризуются повышенной общественной опасностью. О большей общественной опасности анализируемых преступлений свидетельствуют не только специфика их составообразующих признаков (например, развитие высоких технологий обуславливает модификацию «традиционных» и

появление новых способов совершения преступлений), но и особенности механизма преступного поведения в сфере киберпространства: удаленное взаимодействие между участниками преступной деятельности, иные дистанционные и «обезличенные» формы деяния, повышающие «скрытность» преступного поведения; снижение издержек и максимизация криминальных доходов от преступной деятельности (повышение ее эффективности); рост причиняемого имущественного ущерба; снижение рисков привлечения к уголовной ответственности и др. Все это в целом придает имущественным преступлениям, посягающим на новые общественные отношения с помощью высокотехнологичных средств и с использованием современной компьютерной техники, опасные и сложные формы.

**Третий параграф** *«Мошенничество в сфере компьютерной информации в уголовном законодательстве некоторых зарубежных стран»* характеризуется особенностями методологии – юридической компаративистики, используемой в целях обеспечения комплексного анализа нормативных предписаний, содержащихся в ст. 159<sup>б</sup> УК РФ. При этом для уточнения социально-правовой природы анализируемых преступлений исследуются соответствующие положения уголовного законодательства отдельных стран, в том числе представляющих англо-саксонскую и романо-германскую правовые семьи, а также государств-участников СНГ (США, Великобритании, Канады, Республики Сингапур, Новой Зеландии, Содружества Австралии, ФРГ, Швейцарии, Австрии, Португалии, Италии, Испании, Польши, Эстонской Республики, Азербайджанской Республики, Республики Армения, Республики Беларусь, Республики Казахстан, Кыргызской Республики, Республики Молдова, Республики Таджикистан, Республики Узбекистан).

Обобщения зарубежного опыта конструирования уголовно-правовых норм о мошенничестве в сфере компьютерной информации позволяет говорить о самых разных законодательных подходах к установлению уголовной ответственности за рассматриваемые преступления. Как представляется, более точное понимание сущности такого рода деликтов имеет место в современном немецком праве. В § 263а Уголовного кодекса ФРГ «компьютерное» мошенничество определяется как неправомерное нанесение вреда имуществу другого лица в целях противоправного получения имущественной выгоды путем воздействия на результат обработки данных ЭВМ, составляя неправильные программы, используя неправильные или неполные данные, неправомерно применяя данные или влияя на такой процесс каким-либо иным неправомерным воздействием. Предметом преступления, предусмотренного § 263а УК ФРГ, признается имущество в широком смысле слова, а объективная сторона «мошенничества с использованием компьютера» состоит из следующих видов действий: создание неправильных программ, использование неправильных или неполных данных, неправомерное использование данных, неправомерное воздействие на процесс обработки компьютерной информации. Установлено, что отличительной чертой «компьютерного» мошенничества в названных странах романо-германской правовой семьи является то, что оно не

привязано к родовому понятию хищения чужого имущества, а рассматривается как особая разновидность мошенничества или самостоятельный вид имущественного правонарушения в сфере охраны собственности и (или) компьютерной информации.

**Вторая глава** *«Юридическая характеристика преступлений, предусмотренных ст. 159<sup>б</sup> Уголовного кодекса Российской Федерации»* состоит из четырех параграфов и посвящена исследованию особенностей объекта (в том числе предмета), объективной стороны, включая способы и средства совершения рассматриваемых преступлений, субъективных признаков мошенничества в сфере компьютерной информации, а также анализу дифференциации уголовной ответственности за описанные в ст. 159<sup>б</sup> УК РФ преступные посягательства.

**В первом параграфе** *«Особенности объекта преступлений, предусмотренных ст. 159<sup>б</sup> Уголовного кодекса Российской Федерации»* уточняется содержание родового объекта мошенничества в сфере компьютерной информации и в качестве такового соискателем называется цифровая экономика. Другая особенность преступлений, предусмотренных ст. 159<sup>б</sup> УК РФ, заключается в множественности объектов, неразрывно связанных с социально-экономическими, информационно-технологическими и другими общественными отношениями (идея множественности объектов преступлений, предусмотренных ст. 159<sup>б</sup> УК РФ, представляется обоснованной и поддерживается 80 % опрошенных соискателем респондентов). При этом преступные нарушения имущественных прав и интересов в сфере компьютерной информации способны причинять или угрожать причинением как имущественного вреда, так и наступлением общественно опасных последствий вне экономической сферы. Одним из дополнительных объектов преступлений, предусмотренных ст. 159<sup>б</sup> УК РФ, считается информационная безопасность - система отношений, возникающих при осуществлении права на поиск, получение, передачу, производство и распространение информации, применении информационных технологий и обеспечении защиты информации.

Предметом преступлений, описанных в ст. 159<sup>б</sup> УК РФ, признается незаконная имущественная выгода в виде наличных или безналичных денег, электронных денежных средств, иного имущества, в том числе цифровых и иных имущественных прав.

Несмотря на то что компьютерная информация может иметь ценность для собственника имущества и того лица, которое пытается противоправно получить имущественную выгоду посредством использования такой информации, тем не менее компьютерную информацию как таковую нельзя признать предметом преступлений, предусмотренных ст. 159<sup>б</sup> УК. Компьютерная информация лишь отражает (фиксирует) имущественное состояние жертвы. Вместе с тем, если компьютерная информация сама по себе получает легальную (признанную государством) возможность выступать средством платежа, использоваться для обмена на товары, услуги, работы, наличные или безналичные денежные средства, иностранную валюту, то в

таких случаях можно ставить и обсуждать вопрос о признании имеющей стоимостную оценку компьютерной информации предметом имущественного информационного преступления. 58 % опрошенных соискателем респондентов считают, что криптовалюта и цифровая валюта могут выступать предметом преступлений, предусмотренных ст. 159<sup>б</sup> УК РФ.

**Во втором параграфе «Своеобразие объективной стороны преступлений, предусмотренных ст. 159<sup>б</sup> Уголовного кодекса Российской Федерации»** обосновывается, что отличительными признаками объективной стороны преступлений, указанных в ст. 159<sup>б</sup> УК РФ, выступают способ и средства совершения преступного посягательства, связанные с несанкционированным воздействием на компьютерную информацию, использованием компьютерных информационных технологий и технических средств, в том числе средств вычислительной техники, а равно вмешательством в функционирование технических средств, их систем или информационно-телекоммуникационной сети. Результаты социологического опроса показали, что 90 % респондентов к средствам совершения преступлений, ответственность за которые установлена ст. 159<sup>б</sup> УК РФ, относят компьютерную информацию, средства хранения, обработки или передачи компьютерной информации (средства вычислительной техники, электронно-вычислительных машин и/или систем электронных вычислительных машин) и информационно-телекоммуникационную сеть.

Способом совершения преступлений, описанных в ст. 159<sup>б</sup> УК РФ, является неправомерное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационной сети в форме ввода, удаления, блокирования, модификации и иного противоправного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационной сети. Результаты социологического исследования показали, что 68 % опрошенных респондентов согласились с тем, что способом совершения преступлений, предусмотренных ст. 159<sup>б</sup> УК РФ, является вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Вводом компьютерной информации признается неправомерное или неразрешенное законным обладателем внесение (набор) данных (сведений, сообщений) для изменения изначально заданных параметров законного обладателя этих данных (сведений, сообщений). Удаление компьютерной информации представляет собой неправомерное или неразрешенное законным обладателем стирание (устранение) данных (сведений, сообщений) законного обладателя, содержащихся в форме компьютерной информации, из средств ее хранения и обработки. Блокирование компьютерной информации есть полная или частичная временная или постоянная невозможность доступа к данным (сведениям, сообщениям) или использования данных (сведений, сообщений), содержащихся в форме компьютерной информации ее законного обладателя. Ограничение или закрытие доступа к компьютерной информации или к

средствам ее хранения и обработки следует отграничивать от удаления или уничтожения компьютерной информации. По смыслу статьи 159<sup>б</sup> УК РФ, модификация компьютерной информации состоит в совершении действий по неправомерному или без разрешения законного обладателя изменению первоначальных данных (сведений, сообщений), представленных в форме компьютерной информации. Под иным вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей следует понимать такие его формы, как копирование компьютерной информации, передача компьютерной информации, обработка компьютерной информации, нейтрализация средств защиты компьютерной информации, использование вредоносной компьютерной программы, совершение компьютерной атаки или иное неправомерное воздействие программного и (или) программно-аппаратного средства на сервер, средство вычислительной техники (компьютеры) или на информационно-телекоммуникационную сеть.

В параграфе исследуется вопрос о «подвижности» юридического момента окончания преступлений, описанных в ст. 159<sup>б</sup> УК РФ.

**В третьем параграфе** *«Субъективные признаки преступлений, предусмотренных ст. 159<sup>б</sup> Уголовного кодекса Российской Федерации»* сделан вывод о том, что субъективная сторона мошенничества в сфере компьютерной информации выражается в форме прямого умысла. В каждом конкретном случае должно устанавливаться, что лицо, совершившее определенные в диспозиции ст. 159<sup>б</sup> УК РФ действия, заведомо намеревалось использовать доступ к полученной компьютерной информации в целях получения имущественных выгод и причинения имущественного ущерба. При этом признание корыстной цели обязательным элементом преступлений, описанных в ст. 159<sup>б</sup> УК РФ, связано с отказом от узкого понимания ее как цели личного обогащения.

Показано, что общественная опасность «компьютерного» мошенничества очевидна для всякого физического вменяемого лица, достигшего шестнадцатилетнего возраста уголовной ответственности. Нередко совершение рассматриваемых преступлений требует определенных знаний и навыков, однако это не означает, что каждый субъект преступления должен обладать специальным (например, техническим) образованием, так как информационные технологии позволяют действительно передавать криминальный опыт и транслировать его неограниченному кругу лиц. В параграфе получили отражение вопросы криминологической характеристики личности субъектов имущественных преступлений в сфере компьютерной информации.

По итогам проведенного юридико-технического анализа предусмотренные ст. 159<sup>б</sup> УК РФ преступления видятся как новый вид имущественных посягательств в сфере компьютерной информации, которые имеют специфические черты, отличающие их от «традиционных» форм хищений чужого имущества и мошенничества как приобретения права на чужое имущество.

**В четвертом параграфе** *«Дифференциация уголовной ответственности за преступления, предусмотренные ст. 159<sup>б</sup> Уголовного кодекса Российской Федерации»* показано, что указанная статья состоит из четырех частей, в которых описаны преступления небольшой (ч. 1) и средней тяжести (ч. 2), а также тяжкие преступления (ч. 3 и 4).

Особое внимание уделено анализу «компьютерного» мошенничества в отношении банковского счета, а равно в отношении электронных денежных средств. Названный квалифицирующий признак введен в п. «в» ч. 3 ст. 159<sup>б</sup> УК РФ Федеральным законом от 23 апреля 2018 г. № 111-ФЗ. Мошенничество в сфере компьютерной информации, совершенное в отношении банковского счета, а равно в отношении электронных денежных средств, характеризуется особым предметом. Он лишен вещественного содержания и представляет собой безналичные деньги, электронные денежные средства и др. Согласно закону, содеянное в форме хищения чужого имущества квалифицируется по п. «в» ч. 3 ст. 159<sup>б</sup> УК РФ независимо от стоимостного размера предмета преступления.

Единого определения понятия «банковский счет» в федеральном законодательстве не установлено. Исходя из положений главы 45 ГК РФ, банковским счётом является счет, который открывается банком юридическим или физическим лицам (владельцам счета) в целях участия в безналичном денежном обороте, перечислении и выдаче соответствующих сумм со счета, проведении других операций по счету, а также хранения на счёте безналичных денежных средств.

Понятие электронных денежных средств и электронных средств платежа определяется в ст. 3 федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе».

Высокая опасность указанного преступления обусловлена спецификой способа совершения преступления – использованием удаленного доступа к чужому банковскому счету при помощи компьютерных средств, который может быть рассчитан на многократное применение.

**Третья глава** *«Совершенствование уголовного законодательства России об ответственности за мошенничество в сфере компьютерной информации и практики его применения»* состоит из двух параграфов.

**В первом параграфе** *«Совершенствование уголовного законодательства России об ответственности за мошенничество в сфере компьютерной информации»* обращается внимание на несовершенство конструкции ст. 159<sup>б</sup> УК РФ и сосуществование различных доктринальных подходов относительно судьбы «компьютерного» мошенничества. Как представляется, для эффективного уголовно-правового противодействия преступлениям против собственности, совершаемым в сфере компьютерной информации, целесообразно дополнить УК РФ новой статьей 165<sup>1</sup> «Причинение имущественного ущерба путем неправомерного воздействия на объекты в сфере информационно-телекоммуникационной сети и компьютерной информации» и изложить ее в следующей редакции:

«Статья 165<sup>1</sup>. «Причинение имущественного ущерба путем неправомерного воздействия на объекты в сфере информационно-телекоммуникационной сети и компьютерной информации»

1. Причинение имущественного ущерба путем неправомерного воздействия на объекты в сфере информационно-телекоммуникационной сети и компьютерной информации, совершенного с корыстной целью путем использования технических и программных (электронных) средств или устройств, а равно в отношении электронных денежных средств, – 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 двух лет, либо принудительными работами на срок до двух лет, 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, 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 двух 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: а) лицом с использованием своего служебного положения; б) в крупном размере; в) с банковского счета, – 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 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.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, совершенные: а) организованной группой; б) путем компьютерной атаки; в) в особо крупном размере, – наказываются лишением 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.

**Во втором параграфе** «Совершенствование практики применения уголовного законодательства России об ответственности за мошенничество в сфере компьютерной информации» рассмотрены отдельные вопросы

квалификации преступлений, предусмотренных ст. 159<sup>б</sup> УК РФ, и смежных преступных посягательств в сфере отношений собственности и компьютерной информации. На основе обобщения судебной практики по делам о мошенничестве в сфере компьютерной информации предлагается внесение 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». В частности, соискателем обосновывается, что по делам о преступлениях, предусмотренных статьей 159<sup>б</sup> УК РФ, судам следует учитывать положения Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и иного законодательства Российской Федерации, регулирующего отношения по использованию информации, применению информационных технологий и по обеспечению защиты информации».

В заключении обобщаются результаты исследования, формулируются рекомендации по совершенствованию правотворческой и правоприменительной деятельности в сфере уголовно-правового противодействия «цифровым» имущественным преступлениям, определяются перспективы дальнейшей научной разработки темы.

В приложениях содержатся проект постановления Пленума Верховного Суда Российской Федерации «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» (Приложение 1) и форма опросной анкеты (Приложение 2).

### **Основное содержание диссертации отражено в публикациях:**

*Статьи в рецензируемых научных журналах, перечень которых установлен Министерством науки и высшего образования Российской Федерации:*

1. Григорян Г.Р. Юридическая характеристика объекта мошенничества в сфере компьютерной информации // Общество и право. 2017. № 2 (60). С. 54-57.
2. Григорян Г.Р. Особенности способов совершения преступлений, предусмотренных статьей 159.6 Уголовного кодекса РФ // Законодательство. 2017. № 12. С. 55-58.
3. Григорян Г.Р. Об объекте мошенничества в сфере компьютерной информации // Российская юстиция. 2018. № 5. С. 29-31.
4. Григорян Г.Р. Социально-экономические и информационно-технологические основания криминализации мошенничества в сфере компьютерной информации // Юридический вестник Самарского университета. 2019. Т. 5. № 3. С. 141-146.
5. Григорян Г.Р. О социально-правовой сущности корыстных имущественных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Российская юстиция. 2020. № 10. С. 13-15.

6. *Безверхов А.Г., Григорян Г.Р.* Корыстные преступления против собственности в условиях цифровой трансформации // Российская юстиция. 2021. № 1. С. 16-17.

*Научные статьи, опубликованные в иных изданиях:*

7. *Григорян Г.Р.* Мошенничество в сфере компьютерной информации в системе имущественных преступлений // Уголовное право: стратегия развития в XXI веке: материалы XV Международной научно-практической конференции. М.: РГ-Пресс, 2018. С. 406-408.

8. *Григорян Г.Р.* «Цифровые» имущественные преступления: вопросы криминализации и законодательной регламентации // Юридический аналитический журнал. 2021. № 1. С. 73-90.

9. *Григорян Г.Р.* Кража и мошенничество, совершенное с банковского счета, в отношении электронных денежных средств и с использованием электронных средств платежа: вопросы законодательной регламентации и квалификации // Государственная и муниципальная власть в Российской Федерации: современное состояние и перспективы развития: сборник материалов III Всероссийской научно-практической конференции (11 декабря 2020 г.). Чебоксары: ЧКИ РУК, 2021. С. 70-76.