Научная статья
Научная специальность
5.1.4 «Уголовно-правовые науки»

УДК 343.721
DOI https://doi.org/10.26516/2071-8136.2023.3.63

СОЦИАЛЬНО-ПРАВОВАЯ И ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКАЯ ОБУСЛОВЛЕННОСТЬ КРИМИНАЛИЗАЦИИ И ПРОБЛЕМЫ КВАЛИФИКАЦИИ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

© Петрякова Л. А., 2023
Иркутский государственный университет, г. Иркутск, Россия
Байкальский государственный университет, г. Иркутск, Россия

Представлен анализ социально-правовой и информационно-технологической обусловленности криминализации мошенничества в сфере компьютерной информации и некоторых проблем квалификации. Проведенное исследование позволило установить, что социально-правовая обусловленность уголовно-правовой охраны информационной и экономической безопасности является следствием развития цифровой экономики в современном мире. Информационно-технологические факторы обусловленности, в свою очередь, связаны с формированием информационного общества. В свете новых объективных закономерностей необходимо изменить парадигму уголовно-правовой охраны в отношении собственности и сосредоточить внимание на защите имущественных и других экономических отношений в сфере использования информационно-коммуникационных технологий от незаконных вмешательств. Отмечается, что большинство исследователей не поддерживают введение специального состава мошенничества в сфере компьютерной информации. Подчеркивается, что неудачно сформулированная законодательная норма ст. 159^6 УК РФ противоречит традиционному понятию «мошенничества», в результате чего возникают различные проблемы, начиная от поиска в составе мошенничества в сфере компьютерной информации признаков обмана, заканчивая разграничением этого состава с иными составами преступлений, в том числе компьютерными. В результате исследования преступления, предусмотренного ст. 159^6 УК РФ, сделан вывод о нецелесообразности закрепления этого состава в действующем уголовном законе.

Ключевые слова: мошенничество в сфере компьютерной информации, компьютерное мошенничество, кибермошенничество, компьютерная информация, компьютерные преступления.

SOCIO-LEGAL AND INFORMATION-TECHNOLOGICAL CONDITIONS OF CRIMINALIZATION AND PROBLEMS OF QUALIFICATION OF FRAUD IN THE SPHERE OF COMPUTER INFORMATION

© Petryakova L. A., 2023
Irkutsk State University, Irkutsk, Russian Federation
Baikal State University, Irkutsk, Russian Federation

An analysis of the socio-legal and information technology conditionality of the criminalization of fraud in the field of computer information and some qualification problems is presented. The study made it possible to establish that the social and legal conditionality of the criminal law protection of information and economic security is a consequence of the development of the digital economy in the modern world. Information and technological factors of conditionality, in turn, are associated with the formation of the information society. In the light of new objective patterns, it is necessary to change the paradigm of criminal law protection in relation to property and focus on the protection of property and other economic relations in the field of information and communication technologies from illegal interference. It is concluded that the poorly formulated legislative norm of Art. 159^6 of the Criminal Code of the Russian Federation contradicts the traditional concept of "fraud", as a result of which various problems arise, ranging from searching for signs of deception in the composition of fraud in the field of computer information, ending with the distinction between this composition and other elements of crimes, including computer ones. It is noted that most researchers do not support the introduction of a special composition of fraud in the field of computer information. Consistent investigation of the crime under Art. 159^6 of the Criminal Code of the Russian Federation leads to the idea of the uselessness of this composition in the current criminal law.

Keywords: computer information fraud, computer fraud, cyber fraud, computer information, computer crimes.

Введение

За последние годы многие аспекты жизни – от банковских операций до медицинской диагностики – осуществляются при помощи сети Интернет. К сожалению, это стало причиной возникновения нового вида преступности, связанной с использованием компьютерных технологий, среди которых выделяется мошенничество в сфере компьютерной информации.

Своеобразным катализатором здесь стала пандемия 2020 г., которая повлекла за собой масштабный уход в онлайн многих сфер жизнедеятельности общества. Как подчеркнул Президент РФ, за последние шесть лет коли-

чество преступлений, совершенных с использованием информационно-телекоммуникационных технологий, увеличилось более чем в десять раз. С развитием электронной торговли и предоставления услуг в глобальной сети, технологии быстро обновляются, расширяя поле деятельности киберпреступников. Задача государства – эффективно бороться с этим вызовом и защищать граждан и добросовестный бизнес, которые активно используют цифровое пространство. Преступления, совершаемые при помощи информационных технологий, составляют все большую долю в общей структуре преступности, и сегодня их доля достигла 25 %[1].

В настоящем исследовании представлен анализ социально-правовой и информационно-технологической обусловленности криминализации и некоторых проблем квалификации мошенничества в сфере компьютерной информации.

Методика и методология

В основе методологии исследования лежат методы анализа и синтеза, а также сравнительный и логический метод, которые использованы при проведении исследования мошенничества в сфере компьютерной информации. Сравнивалось состояние мошенничества в сфере компьютерной информации в начале и конце исследуемого периода (2012–2022 гг.), а также его отличие от иных составов преступлений. Анализу была подвергнута также совокупность факторов, детерминирующая выявленные изменения.

Использование сравнительного анализа и других указанных методов позволило изучить указанный вид мошенничества, установить обусловленность его криминализации, выявить основные детерминанты, способствующие таким изменениям. На основе полученных результатов предложено исключить из уголовного закона ст. 159[6] УК РФ[2].

Среди методов исследования применялись также статистический метод, метод экспертных оценок, контент-анализ, которые позволили определить динамику состояния рассматриваемого вида мошенничества, особенности его детерминации.

Результаты исследования

Федеральным законом от 29 ноября 2012 г. № 207-ФЗ в Уголовный кодекс Российской Федерации (далее – УК РФ) была введена ст. 159[6] «Мошенничество в сфере компьютерной информации»[3].

Согласно пояснительной записке к проекту федерального закона, введение ст. 159[6] УК РФ было вызвано развитием инвестиционной деятельности, информационных технологий, в том числе в финансовом секторе экономики[4].

Таким образом, одной из главных причин криминализации мошенничества в сфере компьютерной информации является укрепление среди населения доверия к сети Интернет. Пользователи стали размещать в социальных сетях, интернет-магазинах, на веб-сайтах свои личные данные, в том числе данные банковских счетов и карт, которые мошенники похищают и впоследствии используют в своих целях для совершения банковских операций без согласия их владельцев.

Другой причиной криминализации мошенничества в сфере компьютерной информации стала недостаточная урегулированность правоотношений в данной сфере. Таким образом, отсутствие правовых норм, быстрое развитие технологий и популярность сети Интернет создают значительные препятствия для правоохранительных органов в расследовании случаев кибермошенничества.

Согласно официальным данным ГИАЦ МВД РФ, динамика состояния мошенничества в сфере компьютерной информации в России за период с 2012 по 2022 г. выглядит следующим образом (рис.).

Анализ представленных данных за исследуемый период показал, что на территории Российской Федерации количество зарегистрированных мошенничеств, предусмотренных ст. 159[6] УК РФ, имеет тенденцию к снижению (с 2017 по 2022 г.).

Сказанное обусловлено, прежде всего, внесенными изменениями в ст. 159[6] УК РФ, а также разъяснениями, содержащимися в Постановлении Пленума Верховного Суда РФ № 48 (далее – Постановление № 48). Так, например, до 2017 г. мошенничество, совершенное посредством фишинга, социальной инженерии, квалифицировалось как мошенничество в сфере компьютерной информации. Однако п. 21 Постановления № 48 разъяснил, что если хищение чужого

[1] Расширенное заседание коллегии МВД России. URL: http://kremlin.ru/events/president/news/65090 (дата обращения: 19.06.2023).

[2] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 13.06.2023) // КонсультантПлюс: справочная правовая система.

[3] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации : федер. закон от 29 нояб. 2012 г. № 207-ФЗ // Собр. законодательства РФ. 2012. № 49. Ст. 6752.

[4] Пояснительная записка к проекту Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации» // КонсультантПлюс : справочная правовая система.

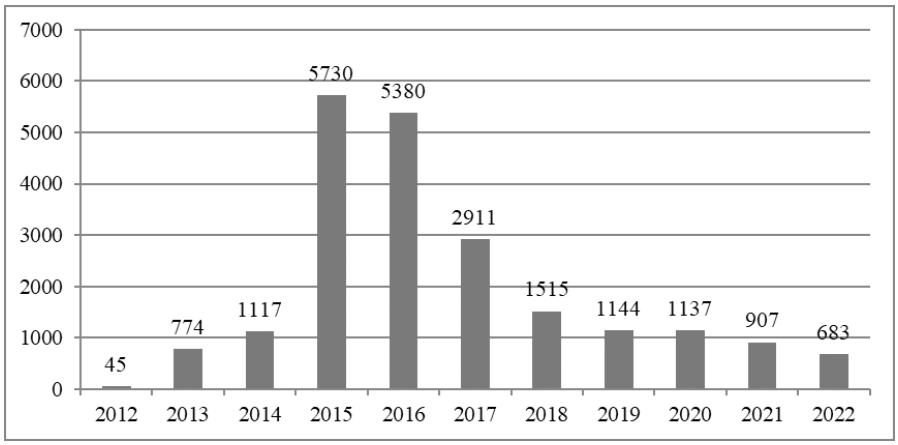

Рис. Динамика абсолютных показателей выявленных случаев мошенничества в сфере компьютерной информации (ст. 159[6] УК РФ), Российская Федерация, 2012–2022 гг.

имущества или приобретение права на чужое имущество осуществляется путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть Интернет (например, создание поддельных сайтов благотворительных организаций, интернет-магазинов, использование электронной почты), то такое мошенничество следует квалифицировать по ст. 159, а не 159[6] УК РФ[1].

Положения, содержащиеся в Постановлении № 48, породили вопрос о возможности применения ст. 159[6] УК РФ, так как случаи мошенничества, которые ранее квалифицировали по рассматриваемой статье, теперь подлежат квалификации по ст. 158 УК РФ. В связи с этим достаточно сложно представить ситуации, когда необходимо вменять состав преступления, предусмотренного ст. 159[6] УК РФ.

Кроме того, организации улучшили свои меры защиты, что позволило снизить количество успешных мошенничеств, а, в свою очередь, киберпреступники переориентировали свою деятельность на другие виды преступлений, свершаемых путем использования информационно-коммуникационных технологий, такие как кража персональных данных и вымогательство.

Появление нового вида мошенничества было неоднозначно воспринято и научным сообществом, породив различные варианты его толкования и квалификации.

Ранее проведенные исследования и анализ судебной практики по поводу мошенничества в сфере компьютерной информации показывают увеличение количества ошибок, связанных с квалификацией рассматриваемых деяний, и доказывают, что дифференциация уголовной ответственности за специальные виды мошенничества была проведена поспешно и непоследовательно.

На сегодняшний день в науке существуют различные точки зрения на то, где должна располагаться рассматриваемая норма.

Так, одни авторы считают, что специальные виды мошенничества следует исключить из Особенной части УК РФ, однако ст. 158, 159, 160 и 163 УК РФ необходимо дополнить квалифицирующим признаком «с использованием информационно-телекоммуникационных технологий» [7, с. 319]. Другие предлагают изменить название ст. 159[6] УК РФ на «Хищение в сфере компьютерной информации» [11, с. 415] или же «Хищение, совершенное с использованием информационно-телекоммуникационных технологий» [12, с. 147]. Противоположной является точка зрения Г. Р. Григоряна, который предлагает ввести в уголовный закон новый состав преступления: «Ст. 165[1]. Причинение имущественного ущерба путем неправомерного воздействия на объекты в сфере информационно-телекоммуникационной сети и компьютерной информации» [6, с. 185–186], декриминализовав при этом п. «г» ч. 3 ст. 158, ст. 159[3], ст. 159[6] УК РФ.

Существует мнение и о целесообразности размещения ст. 159[6] УК РФ в гл. 28 «Преступления в сфере компьютерной информации» [16, с. 196].

Анализ объективной стороны рассматриваемых преступлений показал отступление законодателя от базового принципа соотношения общей и специальной нормы (табл.). В частности, в п. 1 Постановления № 48 указано, что обман и злоупотребление доверием не являются способами хищения чужого имущества или приобре-

[1] О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда Российской Федерации от 30 нояб. 2017 г. № 48 // Рос. газ. 2017. № 280.

Таблица

Сравнение объективной стороны ст. 159 и 159[6] УК РФ

Признаки объективной стороны	**Мошенничество (ст. 159 УК РФ)**	**Мошенничество в сфере компьютерной информации (ст. 159[6] УК РФ)**
Деяние	Хищение имущества или приобретение права на чужое имущество	Хищение чужого имущества или приобретение права на чужое имущество
Способ	Путем обмана или злоупотребления доверием	Путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей
Последствие	Имущественный ущерб собственнику или иному владельцу	Имущественный ущерб собственнику или иному владельцу

тения права на чужое имущество при мошенничестве в сфере компьютерной информации.

Таким образом, ст. 159[6] УК РФ – единственный состав мошенничества, в котором отсутствует ключевой признак этого преступления – обман и злоупотребление доверием. То есть формально исследуемое преступление можно назвать мошенничеством, но на самом деле оно не является им, так как не содержит указанных признаков.

Стоит отметить, что обман и злоупотребление доверием не были включены в рассматриваемый состав преступления с момента его введения. Так, согласно пояснительной записке к проекту федерального закона, мошенничество в сфере компьютерной информации – это хищение или приобретение права на чужое имущество, сопряженное с преодолением компьютерной защиты имущества (имущественных прав) и осуществляемое путем ввода, удаления, модификации или блокирования компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Таким образом, авторы проекта изначально указали, что данное преступление совершается не путем обмана или злоупотребления доверием конкретного субъекта, а путем получения доступа к компьютерной системе.

Сказанное позволяет сделать заключение, что при формулировании ст. 159[6] УК РФ было размыто понятие «мошенничество», так как мошенничество ассоциируется с хищением имущества путем обмана или злоупотребления доверием [8, с. 197].

В связи с этим следует исключить данное преступление из категории мошенничества, так как на самом деле оно не содержит ключевых признаков этого преступления и не может быть к нему отнесено.

Эксперты оценивают введение ст. 159[6] УК РФ по-разному. Некоторые исследователи положительно относятся к этой новации, «независимо от того, являлся ли преступник материально ответственным лицом, а похищаемое имущество было вверенным ему, осуществлялось ли изъятие имущества тайно, такие действия все равно следует квалифицировать по ст. 159[6] УК РФ, если имело место использование компьютерной информации или информационно-коммуникационных сетей» [5].

Другие полагают, что следует исправить возникшую проблему, предлагая различные способы ее решения. В частности, В. Г. Шумихин указал, что «в составе мошенничества в сфере компьютерной информации законодатель не указал способ обмана или злоупотребления доверием, и, таким образом, он представляет собой самостоятельную форму хищения со специфичным способом, отличным от других форм хищения чужого имущества, которая должна быть нормативно урегулирована соответствующим образом» [15, с. 229].

По мнению Ю. О. Алферовой и О. М. Дементьева, в ст. 158 УК РФ следует предусмотреть квалифицирующий признак «хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи

компьютерной информации или информационно-телекоммуникационных сетей» либо ввести самостоятельную статью, которая бы предусматривала ответственность за любые виды хищения с применением компьютерных технологий [1, с. 15]. Однако введение указанного признака в состав кражи не должно включать в себя мошеннический способ, иначе возникнут вопросы при разграничении этих составов.

Существует и предложение о сужении ст. 159⁶ УК РФ путем внесения в качестве обязательного признака «обман или злоупотребление доверием». Так, по мнению Н. А. Лопашенко, «если посмотреть на выделенные выше признаки обмана и злоупотребления доверием, то в ситуациях, когда для завладения чужим имуществом используются возможности компьютерных технологий, часто не сможем отыскать многих из них. Например, при продаже под видом компьютерной игры программы, позволяющей отследить и запомнить доступ к банковскому счету человека, и последующем доступе к этому счету и переводе с него денежных средств на определенный заранее приготовленный преступником счет, нет такого признака мошенничества, как осознанная передача денежных средств преступнику самим потерпевшим навсегда или даже во временное пользование. Потерпевший не подозревает, что используется преступником и будет вынужден расстаться со своими деньгами» [10, с. 604].

Тем не менее большинство авторов указывают на «неудачность самой формулировки в составе мошенничества в сфере компьютерной информации на предмет адресата обмана» [14, с. 230].

Многие исследователи отмечали особенность способа совершения данного состава преступления, который необходимо было бы обозначить самостоятельной формой хищения, что позволило бы решить вопрос о конкуренции ст. 159 и 159⁶ УК РФ [15, с. 231; 3, с. 14].

По мнению Е. А. Ильяшенко, данная норма является мертворожденной, только признание «криптовалют» финансовым активом позволит применять ст. 159⁶ УК РФ по фактам хищения виртуальной валюты [9, с. 53].

Существует и мнение о том, что по своей сути преступление, предусмотренное ст. 159⁶ УК РФ, больше похоже на компьютерное преступление, следовательно, указанную норму необходимо перенести в гл. 28 УК РФ. Это связано с тем, что во всех статьях гл. 28 законодатель использует следующие понятия: уничтожение, блокирование, модификации, копирование компьютерной информации. Возникает закономерный вопрос, а в настоящее время при совершении мошенничества в сфере компьютерной информации нужна ли дополнительная квалификация по ст. 272–274² УК РФ?

Исследователи обращают внимание на то, что за составы компьютерных преступлений предусмотрена более строгая санкция, чем за преступление, предусмотренное ст. 159⁶ УК РФ. Например, в санкции основного состава неправомерного доступа к компьютерной информации (ст. 272 УК РФ) или же нарушения правил эксплуатации (ст. 274 УК РФ) в качестве самого строгого наказания указывается лишение свободы до двух лет, максимальное наказание за совершение мошенничества в сфере компьютерной информации – арест до четырех месяцев. По мнению профессора Н. А. Лопашенко, «это вечная проблема построения согласованных санкций, однако потом, в квалифицированных составах, эта разница в наказании сглаживается, и в конечном итоге именно компьютерное хищение влечет более жесткое наказание, но диспропорция по простым составам есть, и она существенная» [10, с. 607].

Большинство авторов полагают, что в рассмотренной выше ситуации совершенное деяние должно дополнительно квалифицироваться и по ст. 272 или 273 УК РФ [4, с. 15]. По правилам квалификации преступлений такой подход считается неверным, так как если признаки одного преступления полностью входят в число признаков другого, предусматривающего дополнительные признаки, должен применяться только последний состав. Это так называемая законодательно учтенная совокупность преступлений, а нормы, предусмотренные в ст. 272, 274 УК РФ и ст. 159⁶ УК РФ, конкурируют между собой как часть и целое [13, с. 4; 2, с. 115]. Однако, если содеянное квалифицировать только по ст. 159⁶ УК РФ, то мы недооцениваем один из двух пострадавших объектов – либо собственность, либо отношения в сфере компьютерной безопасности – и, следовательно, отказываемся от его охраны. Вывод о применении правил совокупности преступлений также подтверждается сравнительным анализом санкций рассматриваемых норм. Ранее было указано на то, что санкции в ст. 272–273 УК РФ намного строже, чем предусмотренные в ст. 159⁶ УК РФ, что также указывает на необходимость применения правил совокупности преступлений.

Пункт 16 нового Постановления Пленума Верховного Суда № 37 от 15 декабря 2022 г. также указывает на совокупность рассматриваемых норм в ситуации, когда мошенничество в сфере компьютерной информации совершается посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ[1].

Заключение

Подводя итог проведенному исследованию, необходимо констатировать, что мошенничество в сфере компьютерной информации не является типичным видом мошенничества и отличается от него специфическим способом совершения преступления.

Поэтому, в связи с вышесказанным, более правильным было бы исключить ст. 159[6] УК РФ, предусмотрев в составах хищений квалифицирующий признак «использование информационно-коммуникационных технологий».

СПИСОК ЛИТЕРАТУРЫ

1. Алферова Ю. О., Дементьев О. М. Проблемы квалификации компьютерного мошенничества // Science Time. 2014. № 7. С. 11–16.

2. Бархатова Е. Н. Особенности квалификации мошенничества в сфере компьютерной информации и его разграничение с иными составами преступлений // Современное право. 2016. № 9. С. 111–115.

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

4. Болсуновская Л. М. Мошенничество в сфере компьютерной информации: анализ судебной практики // Уголовное право. 2016. № 2. С. 12–16.

5. Вопросы объективной стороны мошенничества в сфере компьютерной информации в судебно-следственной практике / С. Н. Потапкин, А. В. Солдатов, Т. Т. Утешева, Д. А. Данилов // Библиотека научных публикаций Электронного периодического справочника «Система ГАРАНТ». 2015. № 1 (5).

6. Григорян Г. Р. Мошенничество в сфере компьютерной информации: проблемы криминализации, законодательной регламентации и квалификации : дис. ... канд. юрид. наук : 12.00.08 / Самарский национальный исследовательский университет им. академика С. П. Королева. Самара, 2021. 233 с.

7. Ефремова М. А. Уголовно-правовая охрана информационной безопасности : дис. ... канд. юрид. наук : 12.00.08 / Академия Генеральной прокуратуры Российской Федерации. М., 2017. 427 с.

8. Иванченко Р. Б., Малышев А. Л. Проблемы квалификации мошенничества в сфере компьютерной информации // Вестник Воронежского института МВД России. 2014. № 1. С. 194–200.

9. Ильяшенко Е. А. О перспективах привлечения к уголовной ответственности за использование криптовалют в преступных целях // Российский следователь. 2018. № 8. С. 51–54.

10. Лопашенко Н. А. Компьютерное мошенничество – новое слово в понимании хищения или ошибка законодателя? // Пермский юридический альманах. № 2. 2019. С. 598–609.

11. Русскевич Е. А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-телекоммуникационных технологий, и проблемы их квалификации : дис. ... д-ра юрид. наук : 12.00.08 / Моск. ун-т МВД России им. В. Я. Кикотя. М., 2020. 521 с.

12. Фролов М. Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации : дис. … канд. юрид. наук. М., 2018. 211 с.

13. Шарапов Р. Д. Актуальные вопросы квалификации новых видов мошенничества // Проблемы квалификации и расследования преступлений, подследственных органам дознания : материалы Всерос. науч.-практ. конф. Тюмень, 2013. С. 3–5.

14. Шевелева С. В. Мошенничество в сфере компьютерной информации: особенности квалификации и конкуренции со смежными составами преступлений // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2017. № 4 (40). С. 229–234.

15. Шумихин В. Г. Седьмая форма хищения чужого имущества // Вестник Пермского университета. 2014. Вып. 2 (24). С. 229–233.

16. Южин А. А. Мошенничество и его виды в российском уголовном праве : дис. ... канд. юрид. наук : 12.00.08 / Моск. гос. юрид. акад. им. О. Е. Кутафина. М., 2016. 238 с.

REFERENCES

1. Alferova Yu.O., Dementyev O.M. Problemy kvalifikacii kompyuternogo moshennichestva [Problems of qualification of computer fraud]. *Science Time*, 2014, no. 7, pp. 11-16. (in Russian)

2. Barhatova E.N. Osobennosti kvalifikacii moshennichestva v sfere kompyuternoj informacii i ego razgranichenie s inymi sostavami prestuplenij [Features of the qualification of fraud in the field of computer information and its distinction from other crimes]. *Sovremennoe pravo* [Modern law], 2016, no. 9, pp. 111-115. (in Russian)

3. Bezverhov A. Moshennichestvo i ego vidy: voprosy zakonodatelnoj reglamentacii i kvalifikacii [Fraud and its types: questions of legislative regulation and qualification]. *Ugolovnoe pravo* [Criminal law], 2015, no. 5, pp. 8-14. (in Russian)

4. Bolsunovskaya L.M. Moshennichestvo v sfere komp'yuternoj informacii: analiz sudebnoj praktiki [Fraud in the field of computer information: analysis of judicial practice]. *Ugolovnoe pravo* [Criminal law], 2016, no. 2, pp. 12-16. (in Russian)

5. Potapkin S.N., Soldatov A.V., Utesheva T.T., Danilov D.A. Voprosy obyektivnoj storony moshennichestva v sfere kompyuternoj informacii v sudebno-sledstvennoj praktike [Issues of the objective side of fraud in the field of computer information in judicial and investigative practice]. *Biblioteka nauchnyh publikacij elektronnogo yuridicheskogo spravochnika «Sistema Garant»* [Library of scientific publications of the electronic legal reference book "System Garant"], 2015, no. 1 (5). (in Russian)

6. Grigoryan G.R. *Moshennichestvo v sfere komp'yuternoj informacii: problemy kriminalizacii, zakonodatel'noj reglamentacii i kvalifikacii* [Fraud in the field of computer information: problems of criminalization, legislative regulation and qualification. Cand. sci. diss.], Samarskij nacionalnyj issledovatel'skij universitet im. akademika S.P. Koroleva. Samara, 2021, 233 p. (in Russian)

7. Efremova M.A. *Ugolovno-pravovaya ohrana informacionnoj bezopasnosti* [Criminal legal protection of information security. Cand. sci. diss.], Akademiya Generalnoj prokuratury Rossijskoj Federacii. Moskow, 2017, 427 p. (in Russian)

8. Ivanchenko R.B., Malyshev A.L. Problemy kvalifikacii moshennichestva v sfere kompyuternoj informacii [Problems of qualifying fraud in the field of computer information]. *Vestnik Voronezhskogo instituta MVD Rossii* [Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia], 2014, no. 1, pp. 194-200. (in Russian)

[1] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : постановление Пленума Верховного Суда РФ от 15 дек. 2022 г. № 37 // Рос. газ. 2022. № 294.

9. Ilyashenko E.A. O perspektivah privlecheniya k ugolovnoj otvetstvennosti za ispol'zovanie kriptovalyut v prestupnyh celyah [On the prospects of bringing to criminal responsibility for the use of cryptocurrencies for criminal purposes]. *Rossijskij sledovatel'* [Russian investigator], 2018, no. 8, pp. 51-54. (in Russian)

10. Lopashenko N.A. Kompyuternoe moshennichestvo - novoe slovo v ponimanii hishcheniya ili oshibka zakonodatelya? [Computer fraud - a new word in understanding theft or a legislator's mistake?]. *Permskij yuridicheskij al'manah* [Perm legal almanac], no. 2, 2019, pp. 598-609. (in Russian)

11. Russkevich E.A. *Differenciaciya otvetstvennosti za prestupleniya, sovershaemye s ispolzovaniem informacionno-telekommunikacionnyh tekhnologij, i problemy ih kvalifikacii* [Differentiation of responsibility for crimes committed with the use of information and telecommunication technologies, and problems of their qualification. Cand. sci. diss. abstr.], Moskovskij universitet MVD Rossii im. V.YA. Kikotya. Moskow, 2020, 521 p. (in Russian)

12. Frolov M.D. *Ugolovno-pravovoe i kriminologicheskoe protivodejstvie moshennichestvu v sfere kompyuternoj informacii* [Criminal law and criminological counteraction to fraud in the field of computer information. Cand. sci. diss.]. Moskow, 2018, 211 p. (in Russian)

13. Sharapov R.D. Aktualnye voprosy kvalifikacii novyh vidov moshennichestva [Topical issues of qualification of new types of fraud]. *Problemy kvalifikacii i rassledovaniya prestuplenij, podsledstvennyh organam doznaniya: materialy Vseros. nauch.-prakt. konf. Tyumen* [Problems of qualification and investigation of crimes under investigation by bodies of inquiry : materials Vseros. scientific-practical. conf. Tyumen], 2013, pp. 3-5. (in Russian)

14. Sheveleva S.V. Moshennichestvo v sfere kompyuternoj informacii: osobennosti kvalifikacii i konkurencii so smezhnymi sostavami prestuplenij [Fraud in the field of computer information: features of qualification and competition with related crimes]. *Yuridicheskaya nauka i praktika: Vestnik Nizhegorodskoj akademii MVD Rossii* [Legal Science and Practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia], 2017, no. 4 (40), pp. 229-234. (in Russian)

15. Shumihin V.G. Sedmaya forma hishcheniya chuzhogo imushchestva [The seventh form of stealing someone else's property]. *Vestnik Permskogo universiteta*. [Bulletin of the Perm University], 2014, vol. 2 (24), pp. 229-233. (in Russian)

16. Yuzhin A.A. *Moshennichestvo i ego vidy v rossijskom ugolovnom prave* [Fraud and its types in Russian criminal law. Cand. sci. diss.], Mosk. gos. yurid. akad. im. O.E. Kutafina. Moskow, 2016, 238 p. (in Russian)

Статья поступила в редакцию 25.02.2023; одобрена после рецензирования 15.05.2023; принята к публикации 13.09.2023

Received on 25.02.2023; approved on 15.05.2023; accepted for publication on 13.09.2023

Петрякова Людмила Александровна – преподаватель кафедры уголовного права, Иркутский государственный университет (Российская Федерация, 664003, г. Иркутск, ул. К. Маркса, 1); соискатель кафедры уголовного права и криминологии, Институт юстиции, Байкальский государственный университет (Российская Федерация, 664003, г. Иркутск, ул. Ленина, 11), ORCID: 0000-0003-1416-9977, ResearcherID: ABC-1156-2021, SPIN-код: 3607-4003, РИНЦ AuthorID: 1028589, e-mail: poimanowa@mail.ru

Petryakova Lyudmila Aleksandrovna – Teacher of the Department of Criminal Law Law Institute, Irkutsk State University (1, K. Marx st., Irkutsk, 664003, Russian Federation); Competitor of the Department of Criminal Law and Criminology, Institute of State and Law, Baikal State University (11, Lenin st.**,** Irkutsk, 664003, Russian Federation), ORCID: 0000-0003-1416-9977, ResearcherID: ABC-1156-2021, SPIN-код: 3607-4003, RSCI AuthorID: 1028589, e-mail: poimanowa@mail.ru