На правах рукописи

Гайфутдинов Рамиль Рустамович

Понятие и квалификация преступлений против безопасности компьютерной информации

Специальность 12.00.08 – уголовное право и криминология; уголовно-исполнительное право

Автореферат
диссертации на соискание ученой степени
кандидата юридических наук

Казань – 2017

Работа выполнена в ФГАУО ВО «Казанский (Приволжский) федеральный университет»

Научный руководитель:	**Талан Мария Вячеславовна –** доктор юридических наук, профессор, заведующая кафедрой уголовного права ФГАОУ ВО «Казанский (Приволжский) федеральный университет»
Официальные оппоненты:	**Гладких Виктор Иванович –** доктор юридических наук, профессор, заведующий кафедрой уголовного права и процесса ФГБОУ ВО «Государственный университет управления»
	Воробьёв Виктор Викторович – кандидат юридических наук, доцент, заведующий кафедрой уголовного права и криминологии ФГБОУ ВО «СГУ им. Питирима Сорокина»
Ведущая организация:	Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный университет имени М. В. Ломоносова»

Защита состоится 22 декабря 2017 года в 10 часов 00 минут на заседании диссертационного совета Д 212.081.32, созданного на базе ФГАОУ ВО «Казанский (Приволжский) федеральный университет», по адресу: 420008, г. Казань, ул. Кремлевская, д. 18, зал Ученого совета (ауд. 335).

С диссертацией можно ознакомиться в Научной библиотеке им. Н. И. Лобачевского КФУ и на сайте ФГАОУ ВО «Казанский (Приволжский) федеральный университет» (www.kpfu.ru).

Сведения о защите, автореферат и диссертация размещены на официальных сайтах ВАК при Министерстве образования и науки РФ (www.vak.ed.gov.ru) и ФГАОУ ВО «Казанский (Приволжский) федеральный университет» (www.kpfu.ru).

Автореферат разослан «_____» октября 2017 года.

Ученый секретарь
диссертационного совета,
доктор юридических наук, доцент Н. Е. Тюрина

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Современное информационное общество, его экономические, социальные и культурные условия жизни людей во многом обусловливаются уровнем доступности использования информации. При этом определяющее значение в нем приобретают обеспечение права граждан на доступ к информации, соблюдение законности при ее сборе и использовании. Значительная часть информации в настоящее время находится на компьютерных носителях, носит цифровой характер, а государством обозначается переход на качественно новый научно-технологический уровень развития общества. В этих условиях нарушение законов, а тем более любые проявления преступности против безопасности компьютерной информации способны оказывать весьма негативные воздействия на национальную безопасность в целом, развитие науки и техники, а также цифровой экономики в Российской Федерации.

Уголовный кодекс Российской Федерации (далее – УК РФ) хотя и предусматривает достаточно строгие меры уголовно-правовой ответственности за совершение различных видов преступлений против безопасности компьютерной информации (ст.ст. 272-274[1] УК РФ), анализ экспертных данных убеждает в ежегодном росте криминальной активности компьютерной преступности и производного от них размера ущерба[1].

Важно подчеркнуть, что в 2017 г. был принят Федеральный закон № 194-ФЗ о дополнении главы 28 УК РФ статьей 274[1], которая предусматривает серьезные меры ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. Закон вступает в силу с 1 января 2018 г. и в полной мере согласуется с положениями Доктрины (п. 22) о защите информационной инфраструктуры как одной из стратегических целей обеспечения информационной безопасности[2].

---

[1] См. более подробнее: Лацинская М. Group-IB представила отчет о хакерских атаках // Газета.Ру. 2016 г. 13 окт. URL: https://www.gazeta.ru/tech/2016/10/13/10249697/cybercrimecon_2016.shtml (дата обращения: 27.04.2017).

[2] О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона “О безопасности критической информационной инфраструктуры Российской Федерации” : федер. закон Рос. Федерации от 26 июля 2017 г. № 194-ФЗ // Официальный Интернет-портал правовой информации. URL: http://www.pravo.gov.ru (дата обращения: 26.07.2017); Доктрина информационной безопасности Российской Федерации : утв. Указом Президента РФ от 5 дек. 2016 г. № 646 // Собр. законодательства Рос. Федерации. 2016. № 50, ст. 7074.

Названные обстоятельства в своей совокупности обусловливают актуальность проведенного исследования, в котором изучен соответствующий понятийный аппарат, выявлены проблемы применения основ теории квалификации преступлений к деяниям против безопасности компьютерной информации. Учтены актуальные направления политики государства в сфере информатизации общества, уголовно-правовой политики в сфере обеспечения национальной безопасности, а также внесенных изменений в главу 28 УК РФ в последние годы.

Степень научной разработанности темы. По различным проблемам уголовной ответственности за совершение преступлений против безопасности компьютерной информации защищены докторские диссертации В. Г. Степановым-Егиянцем (2016) и Т. М. Лопатиной (2006).

Вопросы уголовной ответственности за рассматриваемые преступления, их отдельные виды и криминологические аспекты исследованы в кандидатских диссертациях С. Ю. Бытко (1998), С. И. Ушакова (2000), М. Ю. Дворецкого (2001), С. Г. Спириной (2001), С. Д. Бражника (2002), А. М. Доронина (2003), А. Ж. Кабановой (2004), А. Е. Шаркова (2004), Т. Л. Тропиной (2005), Д. А. Ястребова (2005), А. В. Геллера (2006), Д. В. Добровольского (2006), М. В. Старичкова (2006), В. Н. Щепетельникова (2006), У. В. Зининой (2007), А. Н. Копырюлина (2007), М. А. Зубовой (2008), А. И. Малярова (2008), Е. А. Маслаковой (2008), А. В. Суслопарова (2010), С. С. Шахрая (2010), И. Г. Чекунова (2013), В. В. Челнокова (2013), А. Н. Ягудина (2013), А. В. Мнацаканян (2016), И. Р. Бегишева (2017) и др.

Отдельные аспекты уголовной ответственности за такие виды преступлений в сочетании с некоторыми проблемами их уголовно-правовой квалификации изучены в кандидатских диссертациях Т. Г. Смирновой (1998), В. В. Воробьева (2000), В. С. Карпова (2002), М. М. Малыковцева (2006).

В то же время специальных исследований, посвященных применению основ теории квалификации преступлений к преступлениям против безопасности компьютерной информации, не проводилось. В этом ракурсе требует также теоретического осмысления и новая норма уголовного права, предусматривающая ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274^1

УК РФ). Она является элементом в уголовно-правовом механизме обеспечения охраны общественных отношений, регулируемых Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Объектом диссертационного исследования выступают общественные отношения, возникающие в связи с квалификацией преступлений против безопасности компьютерной информации, ответственность за которые предусмотрена ст.ст. 272-274[1] УК РФ.

Предметом исследования являются нормы Конституции Российской Федерации, международно-правовых актов, Уголовного кодекса Российской Федерации, иных федеральных законов, уголовного законодательства других государств, материалы статистических данных и специальная литература.

Цель диссертационного исследования – разработка общих и специальных правил квалификации преступлений против безопасности компьютерной информации с учетом нового федерального законодательства, в т.ч. регламентирующего безопасность критической информационной инфраструктуры Российской Федерации.

В соответствии с определенными целями поставлены следующие **задачи**:

- подвергнуть анализу основные положения теории квалификации преступлений и дать их интерпретацию в отношении преступлений против безопасности компьютерной информации;

- раскрыть понятия «компьютерная информация» и «преступление против безопасности компьютерной информации»;

- выявить особенности действующего и прежнего уголовного законодательства об ответственности за рассматриваемые преступления и уяснить специфику их признаков в зарубежных странах;

- установить объективные и субъективные признаки основных и квалифицированных составов преступлений против безопасности компьютерной информации;

- установить специфику преломления общих и специальных правил квалификации преступлений к рассматриваемым видам преступлений.

Методологическую основу диссертационного исследования составляют диалектический метод научного познания, общенаучные (анализ, синтез, дедукция, индукция, исторический, системно-структурный,

статистический, конкретно-социологический) и частнонаучные методы (формально-юридический, историко-правовой, сравнительно-правовой).

Теоретическую основу исследования составляют научные труды по философии, информатике, уголовному праву и криминологии, в том числе по основам теории квалификации преступлений, конституционному, информационному, гражданскому, административному и международному праву таких ученых, как И. Л. Бачило, Ю. М. Батурин, А. Б. Венгеров, В. Б. Вехов, Б. С. Волков, Ю. В. Гаврилин, А. В. Галахова, Л. Д. Гаухман, А. А. Герцензон, В. И. Гладких, В. К. Глистин, В. К. Дуюнов, А. М. Жодзишский, Н. В. Иванцова, Л. В. Иногамова-Хегай, Т. В. Кленова, В. С. Комиссаров, А. В. Корнеева, А. И. Коробеев, Л. Л. Кругликов, В. Н. Кудрявцев, Н. Ф. Кузнецова, А. В. Кубышкин, В. Н. Лопатин, В. П. Малков, А. В. Наумов, А. А. Пионтковский, С. В. Познышев, Т. А. Полякова, А. И. Рарог, Н. Н. Рыбалкин, Р. А. Сабитов, В. С. Савельева, Н. К. Семернева, Б. В. Сидоров, Ф. Р. Сундуров, Н. С. Таганцев, М. В. Талан, И. А. Тарханов, А. Н. Трайнин, И. Я. Фойницкий, А. И. Чучаев, В. А. Якушин, П. С. Яни и др.

Нормативной основой исследования стали Конституция Российской Федерации, международно-правовые акты в сфере охраны компьютерной информации, Модельный уголовный кодекс государств - участников Содружества Независимых Государств, Уголовный кодекс Российской Федерации, Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», иные федеральные законы и подзаконные нормативно-правовые акты в сфере охраны компьютерной информации, уголовные законодательства Армении, Белоруссии, Германии, Грузии, Казахстана, Узбекистана, Украины, Франции.

Эмпирическую основу диссертации составили относящиеся к рассматриваемым в диссертации проблемам постановления Конституционного Суда РФ, постановления Пленума Верховного Суда РФ, статистическая информация Судебного департамента при Верховном Суде РФ за период 2012-2017 гг., а также материалы, опубликованные в средствах массовой информации и информационно-телекоммуникационной сети Интернет.

Автором исследовано 174 судебных акта по делам о преступлениях против безопасности компьютерной информации и компьютерном мошенничестве, постановленных судами общей юрисдикции Центрального, Уральского и Приволжского федеральных округов Российской Федерации в период с 2010 по 2017 годы. Информация по работе с судебными актами приведена в Приложении 1.

Научная новизна исследования выражается в формулировании основных положений теории квалификации преступлений применительно к преступлениям против безопасности компьютерной информации, включая общие и специальные правила квалификации преступлений с учетом наличия межотраслевых связей уголовного и иного законодательств, а также обосновании авторских предложений по совершенствованию уголовного закона и практики его применения. Кроме того, диссертантом впервые проведен уголовно-правовой анализ законодательной конструкции, предусматривающей уголовную ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации, предложены рекомендации по совершенствованию указанного состава преступления, а также выявлены проблемы квалификации и предложены пути их решения.

На защиту выносятся следующие научные положения, выводы и рекомендации:

1. Официальная квалификация преступления как вид правоприменительной деятельности представляет собой *уголовно-правовую оценку* содеянного, осуществляемую в определенной уголовно-процессуальной форме. В структуре обвинения она рассматривается как самостоятельный элемент, наряду с юридической формулировкой, заключающей в себе описание *уголовно-правовых признаков* содеянного. Оба названных элемента связаны между собой, однако отличаются не только по форме, но и по содержанию. Так, в юридической формулировке подлежат описанию все квалифицирующие признаки, однако при ссылке на статью УК РФ указывается точно ее пункт или часть, которые содержат наиболее тяжкий из имеющихся признаков в данном деле. Это позволяет говорить о квалификации преступления в узком и широком смыслах. Понимание квалификации преступления только как содержащуюся в уголовно-процессуальном акте ссылку на пункт, часть и статью УК РФ также имеет теоретическое и законодательное обоснования.

2. Квалификация преступления как одна из *форм* (*разновидностей*) уголовно-правовой квалификации может оказаться одновременно следующим ее *этапом*. Поэтому установление признаков преступления, как процесс отграничения преступного от непреступного, не подлежит включению в содержание процесса квалификации преступления. Она заключается в установлении *вида* совершенного преступления. Юридической основой квалификации преступления является состав преступления как законодательная модель преступления определенного вида (а в определенных случаях – положения Общей части УК РФ, ссылка на которые требуется по специальным правилам квалификации преступления). Предписания других отраслей права, входящих в содержание диспозиции бланкетных норм уголовного права, используются в процессе квалификации преступления при установлении объективных признаков конкретного состава преступления, однако не подлежат включению в ее формулу.

3. Следует различать взаимосвязанные между собой понятия «информационная безопасность», «компьютерная безопасность», «защита информации» и «безопасность информации». При этом компьютерная безопасность рассматривается автором как одна из составляющих информационной безопасности наряду с иными элементами поддерживающей ее инфраструктуры. К ним относятся жилищные, коммунальные системы, системы жизнеобеспечения, средства коммуникации и др. При таком подходе содержание понятия «информационная безопасность» включает в себя компьютерную безопасность.

Защита информации – это урегулированный правом процесс обеспечения информационной безопасности, одной из целей и результатом которого является «безопасность информации». Таким образом, информационная безопасность представляет собой требуемое состояние объекта, которое достигается посредством урегулированной правом защиты информации.

Безопасность информации – это требуемое качество защищенности информации, наличие которого обеспечивает информационная безопасность.

Безопасность обращения компьютерной информации – это отсутствие причинения вреда или его угрозы процессам производства, хранения, использования либо распространения компьютерной информации.

Компьютерная безопасность – это состояние защищенности

компьютерных и сетевых устройств от угроз различного характера.

4. Преступления против безопасности компьютерной информации – это запрещенные уголовным законом Российской Федерации виновно совершенные общественно опасные деяния, причиняющие вред или создающие *угрозу* причинения вреда безопасности *обращения* компьютерной информации или вреда *критической* информационной *инфраструктуре* Российской Федерации.

5. Согласно действующему законодательству, в качестве родового объекта преступлений против безопасности компьютерной информации следует признать общественную безопасность и общественный порядок. При выделении в УК РФ раздела Особенной части УК РФ «Преступления против информационной безопасности» и включения в него деяний, предусмотренных главой 28 действующего закона, как это предлагается в диссертации, родовым объектом уголовно-правовой охраны и преступлений будет являться информационная безопасность. Видовым объектом преступлений против безопасности компьютерной информации является безопасность компьютерной информации, под которой следует понимать состояние защищенности компьютерной информационной сферы, в случае, если ей не наносится вред либо отсутствует реальная угроза его причинения.

6. *Основным непосредственным* объектом уголовно-правовой охраны и преступления, ответственность за которое предусмотрена 1) ст. 272 УК РФ, следует признавать безопасность охраняемой законом компьютерной информации, которая обеспечивается правомерным доступом к ней, 2) ст. 273 УК РФ – безопасность компьютерной информации и средств защиты компьютерной информации, обеспечиваемая правомерным оборотом компьютерных программ и компьютерной информации, 3) ст. 274 УК РФ – безопасность компьютерной информации, компьютерной техники, информационно-телекоммуникационных сетей и оконечного оборудования, обеспечиваемая соблюдением правил их эксплуатации, а также безопасность информационно-телекоммуникационных сетей, обеспечиваемая соблюдением правил доступа к ним, 4) ст. 274^{1} УК РФ – безопасность объектов критической информационной инфраструктуры Российской Федерации.

7. *Предметом* преступных посягательств против безопасности компьютерной информации являются компьютерная информация; вредоносная

компьютерная программа или иная компьютерная информация подобного рода; средства защиты компьютерной информации; средства хранения, обработки или передачи охраняемой компьютерной информации; информационные-телекоммуникационные сети; оконечное оборудование; объекты критической информационной инфраструктуры Российской Федерации; информационные системы; автоматизированные системы управления; сети электросвязи. Вместе с тем следует учитывать, что указанные предметы могут использоваться в том числе и для совершения преступления, т.е. выступать в качестве средств совершения преступления.

8. Вредоносные компьютерные программы либо иную компьютерную информацию подобного рода следует разделять на два вида. *Первый вид* вредоносной компьютерной программы либо иной компьютерной информации подобного рода предназначается для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации (ч. 1 ст. 273 УК РФ). *Второй вид* вредоносной компьютерной программы либо иной компьютерной информации подобного рода предназначается для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации. Первый вид вредоносной компьютерной программы либо иной компьютерной информации подобного рода является более широким понятием по сравнению с содержанием второго вида, которая предназначается исключительно для воздействия на критическую информационную инфраструктуру Российской Федерации.

9. Правильная квалификация содеянного с учетом признаков объективной стороны соответствующих составов преступлений против безопасности компьютерной информации требует единообразия при толковании терминов, используемых в диспозиции уголовно-правовых норм. В связи с этим предлагается под «доступом к компьютерной информации» понимать получение лицом возможности воздействия на компьютерную информацию в виде чтения, записи или исполнения им в компьютерной системе машинных команд.

При квалификации неправомерного доступа к охраняемой законом компьютерной информации, повлекшей ее блокирование (ст. 272 УК РФ),

необходимо учитывать реальную степень общественной опасности такого деяния, зависящую в том числе и от периода фактического блокирования компьютерной информации. Общественно опасным следует признавать содеянное, повлекшее последствия, причинившие существенный вред охраняемым законом правам и интересам. Иные деяния следует признавать малозначительными с учетом положения ч. 2 ст. 14 УК РФ.

Распространение вредоносных компьютерных программ либо иной компьютерной информации подобного рода – это действия, направленные на их обретение неопределенным кругом лиц или выражающиеся в их передаче хотя бы одному лицу.

Под *уничтожением* компьютерной информации следует признавать удаление из памяти компьютерного устройства информации вне зависимости от возможности ее восстановления.

10. Содержание субъективной стороны составов преступлений определяется не только посредством прямого указания на форму вины, но и характеристикой их объективных признаков. Поэтому субъективная сторона основного состава неправомерного доступа к компьютерной информации (ч. 1 ст. 272 УК РФ) характеризуется как умышленной формой вины (прямой и косвенный умысел), так и неосторожностью в виде легкомыслия.

Для преступления, ответственность за которое предусмотрена ч. 2 ст. 274^1 УК РФ, совершаемого с использованием вредоносных компьютерных программ либо иной компьютерной информации подобного рода, характерна только умышленная форма вины в любом ее виде. Легкомыслие как разновидность неосторожности может иметь место в случаях, когда лицом не используются указанные в уголовном законе (в ч. 2 ст. 274^1 УК РФ) средства преступления (т.е. вредоносные компьютерные программы либо иная компьютерная информация подобного рода).

Основные составы создания, использования и распространения вредоносных компьютерных программ либо иной компьютерной информации подобного рода (ч. 1 ст. 273), в т.ч. предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (ч. 1 ст. 274^1), характеризуются виной в форме умысла.

Уголовная ответственность за нарушение правил эксплуатации и доступа к объектам, перечисленным в диспозициях ч. 1 ст. 274 и ч. 3 ст. 274^1 УК РФ,

может наступать только при неосторожной форме вины (по легкомыслию или небрежности).

11. Прерывание преступной деятельности лица на одном из этапов создания или распространения вредоносных компьютерных программ либо иной компьютерной информации подобного рода необходимо квалифицировать как покушение на преступление и квалифицировать содеянное по соответствующей части ст. 273 УК РФ со ссылкой на ч. 3 ст. 30 УК РФ. Создание вредоносных компьютерных программ либо иной компьютерной информации следует признавать оконченным тогда, когда такая программа либо компьютерная информация может быть использована и представляет реальную угрозу.

12. В целях совершенствования уголовного законодательства Российской Федерации и единообразия толкования понятий:

а) внести изменения в 37 статей УК РФ (ст.ст. 63^1, 128^1, 137, 142^1, 147, 159^1, 159^2, 163, 170, 170^1, 170^2, 172^1, 173^1, 173^2, 176, 179, 183, 185^2, 185^3, 185^5, 193^1, 195, 198, 199, 215^4, 275, 276, 283, 283^1, 284, 285^3, 292, 292^1, 310, 311, 320, 354^1), в тексте которых содержатся термины «сообщение», «данные» или «сведения», путем замены их на термин «информация», который эквивалентен содержанию указанных терминов;

б) изложить ч. 1 ст. 138^1 УК РФ «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации» в следующей редакции:

«Незаконные *использование*, производство, приобретение и (или) сбыт специальных технических средств, предназначенных для негласного получения информации, - …» далее по тексту;

в) включить в УК РФ Раздел IX^1 «Преступления против информационной безопасности», перенеся в его содержание преступления, предусмотренные ст.ст. 272-274^1 УК РФ (с учетом предлагаемых нами изменений);

г) наименование главы 28 УК РФ изложить в следующей редакции: «Преступления против безопасности компьютерной информации»;

д) изложить ч. 1 ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» в следующей редакции:

«1. Доступ к охраняемой компьютерной информации, если это деяние повлекло *неправомерно удаление*, блокирование, модификацию либо копирование компьютерной информации, - …» далее по тексту;

е) исключить из ст. 272 УК РФ примечание 1, содержащее определение компьютерной информации;

ж) изложить ч. 1 ст. 273 УК РФ «Создание, использование или распространение вредоносных компьютерных программ» в следующей редакции:

«Создание, использование или распространение компьютерной программы либо иной компьютерной информации, заведомо предназначенной для несанкционированного *удаления*, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, - …» далее по тексту.

Теоретическая значимость исследования определяется разработкой актуальных проблем основ теории квалификации преступлений применительно к преступлениям против безопасности компьютерной информации и формулированием на этой основе новых научных выводов и положений, которые могут быть использованы в дальнейших уголовно-правовых исследованиях по вопросам квалификации преступлений, в том числе против безопасности компьютерной информации.

Практическая значимость работы определяется тем, что сформулированные в ней положения, выводы и рекомендации могут использоваться в практической деятельности правоохранительных органов, в том числе судов, при подготовке постановлений Пленума Верховного Суда Российской Федерации по вопросам квалификации преступлений против безопасности компьютерной информации или других смежных преступлений, а также при подготовке законодательных актов, предусматривающих внесение изменений в Уголовный кодекс Российской Федерации либо иные специальные нормативно-правовые акты, регулирующие общественные отношения в сфере компьютерной безопасности.

Диссертационное исследование может использоваться при подготовке учебных курсов по уголовному праву, в том числе специальных курсов и проведении учебных занятий по вопросам квалификации преступлений против безопасности компьютерной информации.

Достоверность результатов исследования определяется использованием общих и частных методов научного познания, репрезентативной базой статистических данных, солидной эмпирической основой, применением комплексного подхода в раскрытии поставленных целей и задач, значительным количеством новейших законодательных источников, научных работ по проблемам информационной безопасности, квалификации преступлений, учения о преступлениях против безопасности компьютерной информации, материалами судебной практики.

Апробация результатов исследования. Диссертация выполнена на кафедре уголовного права юридического факультета Казанского (Приволжского) федерального университета, где проводились ее рецензирование и обсуждение. Полученные в ходе исследования результаты докладывались диссертантом на Международной научно-практической конференции «Научные воззрения профессоров Пионтковских (отца и сына) и их отражение в современной уголовно-правовой политике» (Казань, 2013), VII Совместном Российско-Германском круглом столе «Преступления в сфере экономики: Российский и Европейский опыт» (Москва, 2015), XIII Международно-практической конференции «Державинские чтения» (Казань, 2017), итоговых научно-практических конференциях профессорско-преподавательского состава Казанского университета в 2014-2016 гг.

Основные положения настоящего исследования отражены в 7 научных статьях автора общим объемом 2,9 п.л., 4 из которых опубликованы в ведущих рецензируемых изданиях, рекомендованных Высшей аттестационных комиссией при Министерстве образования и науки Российской Федерации для публикации результатов диссертационных исследований, общим объемом 1,9 печатных листа.

Результаты исследования используются в учебном процессе при чтении лекций, проведении практических занятий по уголовному праву Российской Федерации на юридическом факультете Казанского (Приволжского) федерального университета.

Структура диссертации определена в соответствии с ею целью, основными задачами, логикой исследования и характером изучаемых проблем. Диссертация состоит из введения, четырех глав, включающих 13 параграфов, заключения, списка сокращений и условных обозначений, списка

использованной литературы и приложения, состоящего из проекта постановления Пленума Верховного Суда Российской Федерации (Приложение 1) и восьми таблиц (Приложение 2-9).

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы диссертационного исследования, показывается степень ее научной разработанности, определяются его объект и предмет, цель и задачи, раскрыты методологическая, теоретическая, нормативная и эмпирическая основы, научная новизна, сформулированы основные положения, выносимые на защиту, раскрываются теоретическая и практическая значимость работы, обоснованность и достоверность результатов исследования, приводятся данные об апробации результатов диссертационного исследования и структура диссертации.

Глава первая «Основные положения теории квалификации преступления и их интерпретация к уголовно-правовой оценке деяния против безопасности компьютерной информации» состоит из трех параграфов. **В § 1.1. «Понятие квалификации преступления, ее виды, содержание и правовые основы»** рассматриваются имеющиеся в уголовно-правовой литературе понятия «квалификации преступления», в основе многих из которых лежит определение, данное В. Н. Кудрявцевым, как «*установление* и *юридическое закрепление* (курсив наш – Р. Г.) точного соответствия между фактическими признаками совершенного деяния и признаками состава преступления, предусмотренного уголовным законом». Автором отмечается, что содержащийся в анализируемом определении признак «юридическое закрепление» не является универсальным, ибо квалификацию преступлений осуществляют не только уполномоченные государством субъекты, но и иные лица, в том числе не имеющие отношения к юриспруденции как профессии. Поэтому соискатель приходит к выводу, что эта составляющая рассматриваемого определения присуща только для характеристики официальной (легальной) квалификации преступления. Указывается, что официальная квалификация преступления как вид правоприменительной деятельности представляет собой *уголовно-правовую оценку* содеянного, осуществляемую в определенной уголовно-процессуальной форме.

Диссертантом утверждается, что установление признаков преступления, как процесс отграничения преступного от непреступного, не подлежит включению в содержание процесса квалификации преступления. Она заключается в установлении *вида* совершенного преступления, поэтому юридической основой квалификации преступления является состав преступления как законодательная модель преступления определенного вида (а в определенных случаях – положения Общей части УК РФ, ссылка на которые требуется по специальным правилам квалификации преступления). Предписания других отраслей права, входящих в содержание диспозиции бланкетных норм уголовного права, используются в процессе квалификации преступления при установлении объективных признаков конкретного состава преступления, однако не подлежат включению в ее формулу.

В § 1.2. «Состав преступления, его виды и алгоритм квалификации преступного деяния» автором анализируются различные подходы к определению состава преступления. Им подчеркивается, что указание на состав преступления как *систему* объективных и субъективных признаков позволяет рассматривать их как взаимосвязанные между собой, что позволяет выявить структуру состава конкретного вида преступления в полном объеме: так, уголовно-правовая характеристика отдельно взятого признака (к примеру, объективного) состава преступления позволяет раскрывать содержание другого (к примеру, субъективного) признака состава преступления. В параграфе рассматриваются классификации составов преступлений, в т.ч. направленных против безопасности компьютерной информации, по оценки степени общественной опасности деяния, особенностям конструирования объективной стороны преступления, внутренней структуры состава преступления.

Далее диссертант признает актуальной проблематику алгоритмизации квалификации преступления по причине отсутствия в литературе устоявшегося мнения к ее решению. Поэтому им обосновывается подход, согласно которому квалификацию преступления следует начинать с установления объектов уголовно-правовой охраны и преступления, далее переходить к установлению объективной стороны состава преступления и совершенного деяния, субъективной стороны состава преступления и деяния, и завершать квалификацию установлением субъекта преступления.

В § 1.3. «Правила квалификации преступления и критерии деления их на виды» автором дан анализ имеющимся в доктрине понятиям «правил квалификации преступлений», что позволило ему под правилами *официальной* квалификации преступлений понимать нормативные, выработанные наукой уголовного права и (или) правоприменительной практикой положения (предписания), определяющие способы (образы) правильной уголовно-правовой оценки квалификатором общественно опасного деяния как конкретного вида преступления в строго определенной процессуальной форме. Автором работы отмечается, что в литературе правила квалификации классифицируются по различным критериям: по количественным и качественным признакам. Однако автор разделяет подход к классификации, предлагаемый А. И. Рарогом, который к общим правилам квалификации преступлений относит правила уголовно-правовой оценки отдельного оконченного преступления, совершенного одним лицом. К ряду специальных правил квалификации преступления – правила квалификации неоконченных преступлений, деяний, совершенных в соучастии, при множественности преступлений, конкуренции уголовно-правовых норм и др., что обусловило дальнейшую структуру исследования преступлений против безопасности компьютерной информации.

Глава вторая «Социально-правовая обусловленность уголовной ответственности за посягательства на безопасность компьютерной информации» состоит из двух параграфов. **В § 2.1. «Понятие компьютерной информации и преступления против ее безопасности»** диссертантом исследованы и сопоставлены между собой понятия «информация», «сведения», «сообщения» и «данные». По завершению этой части параграфа им предлагается в целях единообразия использования и толкования указанных понятий внести изменения в 37 статей УК РФ, в тексте которых содержатся термины «сообщение», «данные» или «сведения», путем замены их на термин «информация», который эквивалентен, по его мнению, содержанию перечисленных понятий в контексте указанных норм.

Во второй части параграфа диссертантом отмечается, что законодателем для определения компьютерной информации в прим. 1 к ст. 272 УК РФ используется только свойство *формы представления* информации, чем обусловлена его пробельность. Им выявлено, что в законодательстве и науке наличествуют два основных подхода к рассматриваемому определению: через

способ обработки такой информации и через форму ее представления. Поэтому автор обосновывает позицию, что исследуемое понятие важно раскрывать, используя оба указанных свойства, и понимать под компьютерной информацией – сведения, представленные в оперируемой техническими средствами форме.

Рассматриваемую в работе группу преступлений (ст.ст. 272-274[1] УК РФ), на взгляд диссертанта, следует именовать как «преступления против безопасности компьютерной информации», под которыми следует понимать запрещенные уголовным законом РФ виновно совершенные общественно опасные деяния, причиняющие вред или создающие опасность причинения вреда безопасности обращения (производства, хранения, использования либо распространения) компьютерной информации или вреда критической информационной инфраструктуре Российской Федерации (далее – КИИ РФ). В предлагаемом определении словосочетание «в сфере» (указанное в УК РФ) заменено другим – «против безопасности». Такая необходимость обусловливается системной структурой Особенной части УК РФ, в котором все посягательства на видовые объекты (за исключением двух, среди которых и анализируемые в работе преступления) определены через термин «против». Ибо безопасность компьютерной информации является конкретно определенным объектом уголовно-правовой охраны в отличие от всеобъемлющего понятия «сфера компьютерной информации». В предлагаемом диссертантом определении акцентируется внимание на видовой и непосредственные объекты уголовно-правовой охраны и преступления.

В § 2.2. «Проблемы криминализации посягательств на безопасность компьютерной информации: сравнительно-правовой аспект» диссертантом раскрываются социально-правовые предпосылки уголовно-правового регулирования отношений в области обеспечения безопасности компьютерной информации, дается краткая справка по внесенным изменениям в гл. 28 УК РФ за весь период действия УК РФ 1996 г., обозначена проблематика регулирования компьютерных преступлений на международном уровне. Особое внимание автором уделено сравнительно-правовому анализу уголовных законодательств Армении, Белоруссии, Грузии, Казахстана, Узбекистана, Украины, а также Германии и Франции.

В качестве позитивного законодательного опыта автором работы отмечается регламентация некоторыми зарубежными странам ответственности

за компьютерный саботаж (Белоруссия, Армения, Германия), изготовления и сбыта специальных средств для получения неправомерного доступа к компьютерной системе или сети (Белоруссия, Армения, Узбекистан, Украина). В параграфе сосредотачивается внимание на положения об усилении уголовной ответственности за посягательства на государственную информационную инфраструктуру в Казахстане и во Франции.

Глава третья «Реализация общих положений теории квалификации преступлений применительно к преступлениям против безопасности компьютерной информации» состоит из пяти параграфов. **В § 3.1. «Особенности установления объекта преступления и предмета посягательства при квалификации содеянного»** отмечается, что в действующем законодательстве родовым объектом составов преступлений, ответственность за которые предусмотрена ст.ст. 272-274[1] УК РФ, является общественная безопасность и общественный порядок. Однако диссертант исходит из того, что родовой объект рассматриваемых преступлений по существу шире обозначенного и им следует признавать информационную безопасность, как один из компонентов обеспечения национальной безопасности государства. О более широком объекте уголовно-правовой охраны, по мнению диссертанта, свидетельствует и непосредственный объект уголовно-правовой охраны ст. 274[1] УК РФ – безопасность КИИ РФ. Поэтому предлагается в Особенной части УК РФ выделить раздел «Преступления против информационной безопасности» и перенести в него главу 28 УК РФ с имеющимися в ней составами преступлений.

В параграфе даны также понятия видового и непосредственных объектов рассматриваемых преступлений. Автором работы также отмечается, что по основному непосредственному объекту уголовно-правовой охраны преступления против безопасности компьютерной информации возможно классифицировать на посягающие на компьютерную информацию общего характера (ст.ст. 272-274 УК РФ) и посягающие на компьютерную информацию, обращающуюся в КИИ РФ (ст. 274[1] УК РФ).

Диссертант анализирует понятие предмета преступления, дает полную характеристику предметам преступлений против безопасности компьютерной информации и раскрывает особенности их установления.

В § 3.2. «Выявление признаков объективной стороны названных составов преступлений и деяний в процессе их квалификации» указывается, что по конструкции объективной стороны рассматриваемые составы преступлений являются сложными. В конструкции составов анализируемых составов преступлений деяния описываются различными способами: 1) как одно действие: «неправомерный *доступ*» (ст. 272); 2) как возможные альтернативные действия: «*создание*, *распространение* и (или) *использование*» (ч.ч. 1 ст. 273 и ст. 274^1); 3) как деяние, выраженное в форме действия или бездействия: «*нарушение* правил» (ст. 274, ч. 3 ст. 274^1), которое представляется возможным совершить также путем смешанного бездействия, когда лицо должно было совершить действие, но совершает действие, которое не должно было совершать; 4) как одно обязательное действие, а другое факультативное: а) неправомерный *доступ* к охраняемой компьютерной информации, содержащейся в КИИ РФ, в том числе с б) *использованием* компьютерных программ либо иной компьютерной информации, предназначенных для неправомерного воздействия на КИИ РФ, или иных вредоносных компьютерных программ (ч. 2 ст. 274^1 УК РФ).

По мнению диссертанта, деяния, описываемые в конструкциях ст.ст. 272-274 УК РФ, и схожие с ними деяния, указанные в ч.ч. 1-3 ст. 274^1 УК РФ, являются особыми формами совершения преступлений, которые позволяют отграничивать один вид посягательства на безопасность компьютерной информации от другого.

Автор обращает внимание на то, что создание (вредоносных компьютерных программ либо иной компьютерной информации подобного рода) можно толковать как определенный процесс и результат, что имеет определенное значение для признания деяния оконченным.

В работе утверждается, что в качестве конструктивного признака *основных* составов преступлений, ответственность за которые предусматривается ч. 1 ст. 272, ч. 1 ст. 274, ч.ч. 2-3 ст. 274^1 УК РФ, выступают последствия. Это придает данным составам вид материальных. В качестве такого рода последствий закон называет уничтожение, блокирование, модификацию либо копирование компьютерной информации (ч. 1 ст. 272); уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб (ст. 274); причинение вреда КИИ РФ (ч.ч. 2-3 ст. 274^1),

характеристики каждого из которых подробно раскрываются в данном параграфе.

Диссертант сгруппировал преступления на основании их отличия по характеру действий, их содержанию и регламентации по следующим видам, связанным 1) с неправомерным доступом к компьютерной информации (ст. 272, ч. 2 ст. 274^1 УК РФ); 2) с созданием, распространением и (или) использованием компьютерных программ либо иной компьютерной информацией (ст. 273, ч. 1 ст. 274^1 УК РФ); 3) с нарушением правил эксплуатации и правил доступа (ст. 274, ч. 3 ст. 274^1 УК РФ).

В § 3.3. «Законодательное описание признаков субъективной стороны составов преступлений и проблемы ее установления в процессе квалификации содеянного» отмечается, что содержание субъективной стороны состава преступления выявляется с учетом способа изложения объективной стороны характеристики в уголовном законе. Методологической основой для установления субъективной стороны преступления в содеянном должны служить объективные поступки людей, отражающиеся в объективной реальности, с правильным установлением фактических обстоятельств дела и соответствующей их интерпретацией. Диссертант, накладывая конструкции форм вины на анализируемые составы преступлений (в отношении некоторых конструкций преступлений удается это сделать только в некоторой степени), делает выводы о характерности той или иной формы вины и ее вида тому или иному преступлению, направленному против безопасности компьютерной информации. Исходя из проведенного анализа, автор делает вывод, что субъективная сторона основного состава неправомерного доступа к компьютерной информации (ч. 1 ст. 272 УК РФ) характеризуется как умышленной формой вины (прямой и косвенный умысел), так и неосторожностью в виде легкомыслия.

Для преступления, ответственность за которое предусмотрена ч. 2 ст. 274^1 УК РФ, совершаемое с использованием вредоносных компьютерных программ (далее – ВКП) либо иной компьютерной информации подобного рода, характерна только умышленная форма вины в любом ее виде. Легкомыслие как разновидность неосторожности может иметь место в случаях, когда лицом не используются указанные в уголовном законе (в ч. 2 ст. 274^1 УК РФ) средства преступления (т.е. ВКП либо иная компьютерная информации).

Основные составы создания, использования и распространения ВКП либо иной компьютерной информации подобного рода (ч. 1 ст. 273), в т.ч. предназначенные для неправомерного воздействия на КИИ РФ (ч. 1 ст. 274^1), характеризуются виной в форме умысла.

Уголовная ответственность за нарушение правил эксплуатации и доступа к объектам, регламентируемая в диспозициях ч. 1 ст. 274 и ч. 3 ст. 274^1 УК РФ, может наступать только при неосторожной форме вины (по легкомыслию или небрежности).

В § 3.4. «Уголовно-правовая характеристика субъекта преступления и его установление в ходе квалификации посягательств против безопасности компьютерной информации» указывается, что особенности, характеризующие деятеля, осуществляющего рассматриваемые преступления, в т.ч. с криминологической стороны, можно вывести из толкования каждой общей нормы, предусматривающей ответственность за все исследуемые виды преступлений. Так, в ч. 1 ст. 272 УК РФ и ч. 2 ст. 274^1 УК РФ, представляется, говорится о деятеле, не обладающем правом доступа к компьютерной информации. Такое обстоятельство имеет важное значение для установления также и формы вины субъекта. Для вменения в вину признаков преступлений, предусмотренных ч. 1 ст. 273 УК РФ либо ч. 1 ст. 274^1 УК РФ, субъект должен обладать совокупностью заранее определенных знаний о предназначенности компьютерной программы или компьютерной информации для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. Такое положение является характерной чертой субъекта. Из толкования ч. 1 ст. 274 УК РФ и ч. 3 ст. 274^1 УК РФ представляется, что нарушить правила может только лицо, на которое возлагаются обязанности по соблюдению определенных правил. Такой подход является общепринятым при анализе конструкции и иных составов преступлений, которыми предусматривается ответственность за нарушение определенных правил.

Однако автор приходит к выводу, что в основных составах преступлений против безопасности компьютерной информации, ответственность за которые предусмотрена ч. 1 ст. 272, ч. 1 ст. 273, ч. 1 и ч. 2 ст. 274^1 УК РФ, субъект преступления не характеризуется какими-либо дополнительными *уголовно-правовыми признаками*, т.е. является общим. Уголовную ответственность за

преступления, ответственность за которые предусматривается ст. 274 и ч. 3 ст. 274^1 УК РФ, может нести лишь специальный субъект, т.е. лицо, обладающее знаниями определенных правил эксплуатации и правил доступа.

В § 3.5. «Особенности уголовно-правовой оценки содеянного при наличии квалифицирующих и особо квалифицирующих признаков составов рассматриваемых преступлений» автором анализируются объективные и субъективные признаки деяния, преобразующие основной состав преступления против безопасности компьютерной информации в квалифицируемый или особо квалифицируемый: причинение крупного ущерба, тяжких последствий либо угрозу их наступления; корыстную заинтересованность; использование служебного положения.

Глава четвертая «Применение специальных правил квалификации преступлений против безопасности компьютерной информации» состоит из трех параграфов. **В § 4.1. «Понятие и квалификация неоконченной преступной деятельности, направленной против безопасности компьютерной информации»** отмечается, что совершение приготовительных действий к преступлениям, ответственность за которые предусмотрена ч. 1 ст. 272, ч. 1 ст. 273 и ч. 1 ст. 274, не является уголовно-наказуемыми деяниями в силу ч. 2 ст. 30 УК РФ. Покушение возможно на любой вид преступления, направленного против безопасности компьютерной информации, за исключением деяний, по конструкции составов преступлений, являющихся формальными преступлениями (ч. 1 ст. 273, ч. 1 ст. 274^1 УК РФ). Однако, по мнению диссертанта, возможно также покушение на создание и распространение ВКП, как состоящих в некоторых случаях из сложных, неодноактных действий. По мнению диссертанта, действия виновных, пресеченных в рамках осуществления ОРМ проверочная закупка, по использованию (в случае фактического использования) и распространению (в случае их передачи сотруднику правоохранительных органов, действующему в рамках ОРМ проверочная закупка) ВКП либо иной компьютерной информации подобного рода, следует считать оконченным преступлением.

В § 4.2. «Особенности квалификации преступлений против безопасности компьютерной информации, совершенных в соучастии» автором анализируются теоретические и практические аспекты (субъективные и объективные) выявления признаков стечения лиц в совместной преступной

деятельности. В данном параграфе диссертантом рассматриваются в том числе и квалифицированные виды преступлений против безопасности компьютерной информации, совершаемые группой лиц по предварительному сговору и организованной группой лиц.

Автором отмечается имеющееся противоречие в ч. 4 ст. 274^1 УК РФ, предусматривающей уголовную ответственность за групповое участие, в том числе и за нарушение правил эксплуатации и правил доступа к объектам КИИ РФ, которому, по мнению диссертанта, характерна только неосторожная форма вины, коим является деяние, описанное в ч. 3 ст. 274^1 УК РФ. Кроме того, автор пришел к выводу, что выявлению на практике при квалификации преступлений всех признаков соучастия препятствует сложность установления фактических данных о личности соучастников в сети Интернет.

В § 4.3. «Квалификация преступлений против безопасности компьютерной информации при их множественности и способы преодоления конкуренции уголовно-правовых норм» соискателем установлено, что рассматриваемые виды преступлений при определенных обстоятельствах образуют различные виды совокупности преступлений (реальную и идеальную). В параграфе подвергаются анализу наиболее часто встречающие примеры из судебной практики по квалификации преступлений, видовыми объектами которых являются конституционное право гражданина на личную тайну (гл. 19), собственность (гл. 21), сфера экономической деятельности (гл. 22), по совокупности с преступлениями против безопасности компьютерной информации.

Автором констатируется, что в литературе и судебной практике нет единого подхода к вопросу о необходимости квалификации по совокупности преступлений, ответственность за которые предусмотрена ст.ст. 159^6 и 272 УК РФ. Поэтому им обоснован тезис о том, что ответственность по указанным статьям предусмотрена за совершение различных противоправных действий, с учетом различной их объективной стороны. Диссертантом утверждается, что при квалификации деяния, имеющего все признаки компьютерного мошенничества, путем удаления, блокирования, модификации либо копирования компьютерной информации, необходимо установить наличие либо отсутствие неправомерного доступа к охраняемой законом компьютерной информации. Если признаки указанного состава преступления (ст. 272) установлены (в рамках последствий,

наступивших в результате компьютерного мошенничества), то необходима квалификация таких действий лица в качестве идеальной совокупности преступлений, ответственность за которые установлена соответствующими частями ст.ст. 159^6 и 272 УК РФ.

В параграфе акцентируется внимание на то, что в главу 28 УК РФ введена по своей норма (ст. 274^1), конкурирующая при квалификации преступлений с другими видами преступлений против безопасности компьютерной информации (ст.ст. 272-274), как общие нормы (ст.ст. 272-274) и специальные нормы (ч. 1-3 ст. 274^1) составов самостоятельных преступлений. Поэтому при наличии в преступлении всех признаков специальной нормы, квалификация преступления должна производиться соответственно по специальной норме (соответствующей части ст. 274^1), как учитывающая наиболее полно все признаки состава преступления.

Заключение содержит основные выводы и предложения по теме диссертационного исследования, определяются дальнейшие направления исследования.

В **приложениях** представлены проект постановления Пленума Верховного Суда Российской Федерации «О судебной практике по делам о преступлениях против безопасности компьютерной информации», таблицы работы с судебными актами, анализа использования категориального (понятийного) аппарата в УК РФ, а также таблицы со статистическими сведениями о преступности против безопасности компьютерной информации.

ОСНОВНЫЕ НАУЧНЫЕ РЕЗУЛЬТАТЫ ДИССЕРТАЦИИ ОПУБЛИКОВАНЫ В СЛЕДУЮЩИХ РАБОТАХ:

Публикации в журналах, входящих в Перечень российских рецензируемых научных журналах, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученых степеней доктора и кандидата наук:

1. *Талан, М. В., Гайфутдинов, Р. Р.* Уголовно-правовая охрана компьютерной информации // Вестник экономики, права и социологии. – 2011. – № 4. – С. 197-201. (доля авторства – 80%) – 0,36 п.л.

2. *Гайфутдинов, Р. Р.* Уголовно-правовая характеристика посягательств на персональные данные, обрабатываемые в автоматизированных

системах // Ученые записки Казанского университета. Серия Гуманитарные науки. – 2014. – Т. 156, кн. 4. – С. 158-165. – 0,52 п.л.

3. *Гайфутдинов, Р. Р.* К вопросу о типологии личности компьютерных преступников с учетом характера и мотивации их криминальной деятельности // Вопросы российского и международного права. – 2017. – Том 7. № 4А. – С. 245-256. – 0,63 п.л.

4. *Гайфутдинов, Р. Р.* Типы компьютерных мошенников // Вестник экономики, права и социологии. – 2017. – № 2. – С. 54-58. – 0,46 п.л.

Публикации в иных изданиях:

5. *Гайфутдинов, Р. Р.* Проблема реформирования уголовного законодательства России об ответственности за преступления в сфере компьютерной информации // Научные воззрения профессоров Пионтковских (отца и сына) и современная уголовно-правовая политика / Под ред. Профессоров Ф. Р. Сундурова и М. В. Талан. – М.: Статут, 2014. – С. 241-244. – 0,19 п.л.

6. *Гайфутдинов, Р. Р.* Определение понятий компьютерной информации и компьютерных преступлений в уголовном законе // Сборник аспирантских научных работ юридического факультета / Казанский (Приволжский) федеральный университет; под ред. З. Ф. Хусаинова. – Казань, 2014. – Вып. 15. – С. 32-38. – 0,32 п.л.

7. *Гайфутдинов, Р. Р.* Компьютерные преступления против собственности по законодательству Российской Федерации и Германии // Преступления в сфере экономики: российский и европейский опыт: материалы VII Совместного российско-германского круглого стола, Москва, 26 октября 2015 г. / ред. кол.: А. И. Рарог, Т. Г. Понятовская. – М.: Издательский центр Университета О. Е. Кутафина (МГЮА), 2016. – С. 64-72. – 0,51 п.л.