На правах рукописи

Бегишев Ильдар Рустамович

ПОНЯТИЕ И ВИДЫ ПРЕСТУПЛЕНИЙ В СФЕРЕ ОБРАЩЕНИЯ ЦИФРОВОЙ 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 на кафедре уголовного права и процесса частного образовательного учреждения высшего образования «Казанский инновационный университет имени В. Г. Тимирясова (ИЭУП)».

Научный руководитель: **Бикеев Игорь Измаилович,**
доктор юридических наук (12.00.08), профессор, заслуженный юрист Республики Татарстан, первый проректор, проректор по научной работе, профессор кафедры уголовного права и процесса ЧОУ ВО «Казанский инновационный университет имени В. Г. Тимирясова (ИЭУП)»

Официальные оппоненты: **Лопатина Татьяна Михайловна,**
доктор юридических наук (12.00.08), профессор, заведующий кафедрой права ФГБОУ ВО «Смоленский государственный университет»

Чупрова Антонина Юрьевна,
доктор юридических наук (12.00.08), доцент, профессор кафедры уголовного права и криминологии ФГБОУ ВО «Всероссийский государственный университет юстиции (РПА Минюста России)»

Ведущая организация: **ФГАОУ ВО «Северо-Кавказский федеральный университет»**

Защита состоится 6 октября 2017 года в 11 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, 18, ауд. 335 (зал заседаний диссертационного совета).

С диссертацией можно ознакомиться в научной библиотеке имени Н. И. Лобачевского ФГАОУ ВО «Казанский (Приволжский) федеральный университет» и на официальном сайте ФГАОУ ВО «Казанский (Приволжский) федеральный университет» (http://kpfu.ru).

Сведения о защите и цифровая версия автореферата диссертации размещены на официальных сайтах ВАК при Минобрнауки России (http://vak.ed.gov.ru) и ФГАОУ ВО «Казанский (Приволжский) федеральный университет» (http://kpfu.ru).

Автореферат разослан 6 июля 2017 года.

Ученый секретарь
диссертационного совета Д 212.081.32
доктор юридических наук, доцент Н.Е. Тюрина

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертационного исследования. Развитие глобального информационного общества оказывает значительное влияние на будущее России, в том числе на увеличение технологического и промышленного потенциала страны, на решение стоящих перед ней экономических и социальных задач, на укрепление ее обороноспособности и национальной безопасности. Достижения науки и техники, с одной стороны, дают возможность создания современных информационно-телекоммуникационных устройств, систем и сетей с огромным потенциалом, а с другой – процесс их использования и совершенствования повлек за собой ряд негативных явлений, таких как рост преступлений в сфере обращения информации.

В Доктрине информационной безопасности Российской Федерации говорится о возрастании масштабов компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличении числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее[1].

Хотя вопросы ответственности за преступления в сфере компьютерной информации разрабатываются в нашей стране и за рубежом уже несколько десятилетий, тем не менее об их окончательном решении говорить не приходится. По отдельным вопросам такой проблематики существуют различные точки зрения. В теории уголовного права пока нет однозначного понимания цифровой информации как предмета преступления, недостаточно учтено развитие терминологии в сфере обращения цифровой информации, существуют пробелы в уголовном законодательстве в части ответственности за новейшие высокотехнологичные деяния в сфере обращения цифровой информации.

Опасность таких преступлений обусловлена не только масштабами пагубных воздействий, например, результатами посягательств на критически важные и потенциально опасные информационные инфраструктуры, но и ростом

[1] См.: Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации // СЗ РФ. 2016. № 50. Ст. 7074.

их количества. Так, в 1997 г. российскими органами внутренних дел было зарегистрировано лишь 23 преступления в сфере компьютерной информации, а в 2016 г. – уже 1748[2]. Следует отметить, что приведенные данные не в полной мере соответствуют реальному положению дел в связи с высокой латентностью указанных преступлений.

Уголовно-правовая наука должна отражать потребности времени, учитывать развитие и состояние научно-технического прогресса, что, на наш взгляд, в настоящее время не реализовано в достаточной мере при уголовно-правовом регулировании отношений в сфере обращения цифровой информации.

Вышесказанное свидетельствует о необходимости комплексного изучения понятия и видов преступлений в сфере обращения цифровой информации, и, следовательно, об актуальности избранной для диссертационного исследования темы.

Степень научной разработанности темы исследования. Проблемы исследования информации, в том числе компьютерной, в качестве предмета преступления и объекта уголовно-правовой охраны нашли отражение в диссертационных исследованиях Р. Г. Асланяна (2016), М. А. Зубовой (2008), В. В. Челнокова (2013), И. А. Юрченко (2000), С. А. Яшкова (2005) и др.

Уголовно-правовые, организационно-правовые и криминологические аспекты преступлений в сфере компьютерной информации изучались в кандидатских работах Р. К. Ахметшина (2006), В. А. Бессонова (2000), С. Д. Бражника (2002), С. Ю. Бытко (2002), В. В. Воробьева (2000), М. С. Гаджиева (2004), М. Ю. Дворецкого (2001), Д. В. Добровольского (2006), Р. И. Дремлюги (2007), А. С. Егорышева (2004), А. А. Жмыхова (2003), У. В. Зининой (2007), Д. А. Зыкова (2002), А. Ж. Кабановой (2004), В. С. Карпова (2002), А. А. Комарова (2011), А. Н. Копырюлина (2007), С. С. Медведева (2008), С. С. Наумова (2001), О. М. Сафонова (2015), Т. Г. Смирновой (1998), С. Г. Спириной (2001), М. В. Старичкова (2006), А. В. Суслопарова (2010), С. И. Ушакова (2000), З. И. Хисамовой (2016), С. С. Шахрая (2010) и некоторых других исследователей.

Среди работ, направленных на исследование мер противодействия

[2] См.: Статистика и аналитика // Официальный сайт МВД России. [Электронный ресурс]. – URL: https://mvd.ru/Deljatelnost/statistics (дата обращения: 16.01.2017).

неправомерному доступу к компьютерной информации (далее – НДКИ), отметим диссертационные исследования Р. М. Айсанова (2006), А. М. Доронина (2003), К. Н. Евдокимова (2006), Д. Г. Малышенко (2002), М. А. Простосердова (2016), И. А. Сало (2011), В. П. Числина (2004), А. Е. Шаркова (2004), Д. А. Ястребова (2005) и некоторых других ученых.

Исследованию уголовной ответственности за оборот вредоносных компьютерных программ (далее – ВКП) и нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (далее – НПЭ) посвящены кандидатские исследования М. М. Малыковцева (2006), Е. А. Маслаковой (2008), А. Н. Ягудина (2012) и других исследователей.

Проблемы, возникающие в связи с совершением преступлений в сфере электронной информации, рассматривались в диссертациях А. В. Геллера (2006), А. И. Малярова (2008), В. П. Щепетильникова (2006) и др.

Обеспечению информационной безопасности уголовно-правовыми средствами и противодействию информационному терроризму посвящены кандидатские диссертации А. С. Изолитова (2008), Д. А. Калмыкова (2005), Д. А. Ковлагиной (2016), Е. В. Красненковой (2006), А. В. Мнацаканян (2016) и других ученых.

Изучению проблем киберпреступности, ее криминологически значимых аспектов, а также мер уголовно-правовой борьбы с ней посвящены кандидатские диссертации Т. Л. Тропиной (2005), И. Г. Чекунова (2013) и других авторов.

Также отметим, что противодействию преступлениям в сфере компьютерной информации и правовому обеспечению информационной безопасности посвящены докторские диссертационные исследования Л. А. Букалеровой (2006), В. Б. Вехова (2008), Ю. В. Гаврилина (2000), Н. Н. Куняева (2010), Т. М. Лопатиной (2006), В. А. Мещерякова (2001), А. Л. Осипенко (2010), Т. А. Поляковой (2008), В. Г. Степанова-Егиянца (2016), А. Ю. Чупровой (2015) и других ученых.

В то же время особую значимость для решения поставленных в диссертации задач имеют труды ученых различных специальностей, в которых, в частности, освещались отдельные аспекты правового режима информации, информационной безопасности, защиты информации и информационной инфраструктуры.

К числу таких авторов относятся Г. А. Атаманов, О. Я. Баев, Ю. М. Батурин, И. Л. Бачило, И. Ю. Богдановская, В. А. Герасименко, В. А. Голубев, В. М. Елин, А. К. Жарова, С. В. Зарубин, П. Д. Зегжда, Н. А. Зигура, А. Г. Кибальник, П. У. Кузнецов, В. Н. Лопатин, Н. А. Лопашенко, А. В. Лукацкий, А. А. Малюк, А. В. Минбалеев, А. В. Морозов, В. Б. Наумов, С. А. Петренко, Т. А. Полякова, Е. Р. Россинская, В. А. Садовничий, Е. С. Саломатина, С. В. Скрыль, Е. В. Старостина, А. А. Стрельцов, Э. В. Талапина, О. В. Танимов, А. М. Тарасов, А. А. Тедеев, Л. К. Терещенко, М. И. Третьяк, Р. М. Узденов, А. А. Хорев, В. Н. Черкасов, Г. И. Чечель, В. П. Шерстюк, А. Н. Яковлев и др.

Однако проведенные исследования, несмотря на их несомненную ценность, не решили многие вопросы, имеющие существенное значение для уголовного права и практики применения уголовного законодательства и отмеченные при обосновании актуальности темы диссертационного исследования.

Объектом исследования являются общественные отношения, складывающиеся по поводу уголовно-правовой регламентации преступлений в сфере обращения цифровой информации.

Предметом исследования выступают нормы Конституции Российской Федерации, международно-правовых актов, уголовного законодательства Российской Федерации и некоторых зарубежных стран, федерального законодательства, регулирующие отношения в информационной сфере, статистические данные о преступлениях в сфере компьютерной информации, материалы экспертно-аналитических отчетов в области информационной безопасности, материалы судебной практики, касающиеся применения уголовно-правовых норм об ответственности за преступления в сфере компьютерной информации, специальная литература и интернет-ресурсы информационно-телекоммуникационной сети (далее – ИТКС) «Интернет», посвященные различным проблемам противодействия преступлениям в сфере компьютерной информации.

Цель и задачи исследования. Целью исследования является установление уголовно-правовой природы преступлений в сфере обращения цифровой информации и выработка обоснованных предложений по совершенствованию и повышению эффективности уголовного законодательства об ответственности за отдельные виды таких деяний и практики его применения.

Цель исследования определила постановку и решение следующих **задач:**

– раскрыть содержание цифровой информации и дать ее научное определение;

– определить понятие преступлений в сфере обращения цифровой информации;

– обосновать и внести предложения по совершенствованию уголовной ответственности за такие преступления, как неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных компьютерных программ; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей; мошенничество в сфере компьютерной информации; незаконный оборот специальных технических средств, предназначенных для негласного получения информации (далее – СТС НПИ);

– разработать и обосновать предложения об установлении уголовной ответственности за посягательства на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объектов; за незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации; за приобретение или сбыт цифровой информации, заведомо добытой преступным путем.

Методологическую основу диссертационного исследования составляют общенаучные методы – диалектический, формальной логики, анализа и синтеза; частнонаучные методы – логико-юридический, сравнительно-правовой, системно-структурный, анализа документов; социологические методы, в том числе метод экспертных оценок, анкетирование, анализ печатных и электронных изданий, статистические методы.

Теоретическую основу диссертационного исследования составляют труды отечественных и зарубежных авторов по уголовному и информационному праву, информационной безопасности и защите информации: Р. М. Айсанова, И. И. Бикеева, Л. А. Букалеровой, С. Ю. Бытко, В. Б. Вехова, А. Г. Волеводза, А. А. Гребенькова, О. В. Григорьева, Д. В. Добровольского, К. Н. Евдокимова, М. А. Ефремовой, У. В. Зининой, Н. В. Иванцовой, А. Ж. Кабановой, В. С. Карпова, Т. В. Кленовой, О. Н. Крапивиной, Е. В. Красненковой, Л. Л. Кругликова, Н. Н. Куняева, С. П. Кушниренко, Т. М. Лопатиной,

В. П. Малкова, А. И. Малярова, Е. А. Маслаковой, С. С. Медведева, В. А. Мещерякова, А. В. Мнацаканян, Н. Г. Муратовой, А. И. Рарога, Д. Прокиса, Б. В. Сидорова, Б. Скляра, В. Г. Степанова-Егиянца, Ф. Р. Сундурова, М. В. Талан, И. А. Тарханова, Т. Л. Тропиной, А. Ю. Чупровой, А. И. Чучаева, Г. А. Шагинян, В. Н. Щепетильникова, И. А. Юрченко, В. А. Якушина, С. А. Яшкова и др.

Нормативно-правовую базу диссертационного исследования составляют Конституция Российской Федерации, международно-правовые акты, относящиеся к данной сфере, Уголовный кодекс Российской Федерации (далее – УК РФ), федеральные законы, акты Президента и Правительства Российской Федерации, другие отечественные и зарубежные нормативные правовые акты.

Эмпирическую базу диссертационного исследования составляют:

– постановления Конституционного Суда Российской Федерации;

– данные анализа 158 приговоров, вынесенных судами за период с 2006 по 2016 г. и размещенных в открытом доступе на сайтах Государственной автоматизированной системы Российской Федерации (далее – ГАС РФ) «Правосудие» и справочно-правовой системы по судебным решениям (далее – СПС) «РосПравосудие» на территории 5 республик (Башкортостан, Дагестан, Саха (Якутия), Татарстан, Удмуртская), 2 краев (Красноярский, Ставропольский), 11 областей (Астраханская, Кировская, Костромская, Московская, Оренбургская, Самарская, Саратовская, Свердловская, Смоленская, Тамбовская, Томская), 1 автономного округа (Ямало-Ненецкий) по уголовным делам о преступлениях, предусмотренных ст. 272, 273, 274 УК РФ;

– статистические данные МВД России о количестве зарегистрированных преступлений в сфере компьютерной информации в Российской Федерации за период с 1997 по 2016 г.;

– экспертно-аналитические отчеты российских и зарубежных компаний, специализирующихся на обеспечении информационной безопасности и защиты информации (InfoWatch, Group-IB, Trustwave, G Data Software и др.), а также аналитические материалы ведущих антивирусных компаний (Лаборатория Касперского, Dr.Web, McAfee и др.) за период с 2010 по 2016 г.;

– результаты анкетирования 175 респондентов: сотрудников соответствующих профилю диссертации подразделений МВД России, СК России, ФСБ России и ФСО России; преподавателей юридических факультетов и вузов; ученых,

исследующих различные вопросы обеспечения информационной безопасности; работников организаций, занимающихся практической реализацией мер по защите информации (97 экспертов на территории Республики Татарстан и 78 онлайн-экспертов в ИТКС «Интернет»).

Научная новизна диссертационного исследования заключается в исследовании цифровой информации как предмета преступления, в выявлении проблем и спорных положений уголовно-правовой регламентации преступлений в сфере обращения цифровой информации, в обосновании авторских предложений по дополнению, совершенствованию и повышению эффективности уголовного закона и практики его применения.

Научная новизна исследования нашла свое отражение в следующих основных **положениях, выносимых на защиту:**

1. Предметом преступления, посягающего на информацию, обращающуюся в информационно-телекоммуникационных устройствах, их системах и сетях, следует признавать не компьютерную, а цифровую информацию.

В примечании 1 к ст. 272 УК РФ предлагаем дать определение понятия «цифровая информация» вместо более узкого и менее точного понятия «компьютерная информация» в следующей авторской редакции:

«Под цифровой информацией понимаются сведения (сообщения, данные), обращающиеся в информационно-телекоммуникационных устройствах, их системах и сетях».

Учитывая, что термин «цифровая информация» является более полным и точным, чем термин «компьютерная информация», рекомендуем использовать его в соответствующих статьях Особенной части УК РФ и отразить указанное понятие в ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. В целях упорядочения терминологии, обеспечения единства и системности уголовного законодательства, основываясь на понятиях, используемых в федеральном законе, регулирующих отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, при применении информационных технологий, а также при обеспечении защиты информации целесообразно использовать более широкий по содержанию термин «информационно-телекоммуникационные

устройства, их системы и сети» в статьях Особенной части УК РФ вместо предусмотренного в ст. 274 УК РФ термина, указывающего на объекты обращения цифровой информации в виде «средств хранения, обработки или передачи компьютерной информации и ИТКС».

3. Под преступлением в сфере обращения цифровой информации предложено понимать предусмотренное уголовным законом виновно совершенное общественно опасное деяние, направленное на нарушение конфиденциальности, целостности, достоверности и доступности охраняемой законом цифровой информации.

При этом защищаемыми свойствами цифровой информации ограниченного доступа являются ее конфиденциальность, целостность и достоверность, а общедоступной информации – ее целостность, достоверность и доступность.

4. Поскольку ИТКС «Интернет» содержит интернет-ресурсы, размещающие информацию о способах совершения преступлений в сфере компьютерной информации, а также объявления о предоставлении незаконных услуг в этой сфере, предлагается в порядке предупреждения этих преступлений ввести механизм внесудебного ограничения доступа на территории Российской Федерации к такой информации, дополнив п. 1 ч. 5 ст. 15.1 «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» следующим пунктом:

«е) информации о способах совершения преступлений в сфере цифровой информации, а также объявлений по предоставлению незаконных услуг в этой сфере».

5. Поскольку общественная опасность неправомерного доступа к цифровой информации близка по своей сути и общественной опасности перехвату цифровой информации в пространстве и в связи с отсутствием в УК РФ нормы, предусматривающей ответственность за перехват цифровой информации, предлагается включить упоминание о данном деянии в наименование ст. 272 УК РФ и в диспозицию ч. 1 ст. 272 УК РФ, изложив ее в следующей авторской редакции:

«Статья 272. Неправомерный доступ к охраняемой законом цифровой информации или ее перехват

1. Неправомерный доступ к охраняемой законом цифровой информации, а равно незаконный ее перехват, если это деяние повлекло уничтожение, блокирование, модификацию, копирование цифровой информации либо ознакомление с ней, нарушение работы информационно-телекоммуникационных устройств, их систем и сетей, –

наказывается ... (далее по тексту УК РФ)*».*

В примечании 3 к ст. 272 УК РФ предлагаем дать определение понятия «перехват цифровой информации» в следующей редакции:

«Под перехватом цифровой информации понимается процесс неправомерного ее получения с использованием специального технического средства, предназначенного для обнаружения, приема и обработки электромагнитного излучения в пространстве».

6. Ввиду уточнения термина, указывающего на объекты обращения цифровой информации, обосновано предложение об изложении наименования ст. 274 УК РФ и диспозиции ч. 1 ст. 274 УК РФ в следующей авторской редакции:

«Статья 274. Нарушение правил эксплуатации или иное нарушение работы информационно-телекоммуникационных устройств, их систем и сетей

1. Нарушение правил эксплуатации или иное нарушение работы информационно-телекоммуникационных устройств, их систем и сетей, повлекшее уничтожение, блокирование, модификацию либо копирование охраняемой законом цифровой информации, причинившее крупный ущерб, –

наказывается ... (далее по тексту УК РФ)*».*

7. Поскольку деяния, предусмотренные ст. 272, 273, 274 УК РФ, представляют собой единую систему преступлений, посягающих на цифровую информацию, то гл. 28 УК РФ предлагается назвать «Преступления в сфере обращения цифровой информации», а ст. 272, 273 и 274 УК РФ озаглавить как «Неправомерный доступ к цифровой информации или ее перехват», «Создание, использование и распространение вредоносных цифровых программ» и «Нарушение правил эксплуатации или иное нарушение работы информационно-телекоммуникационных устройств, их систем и сетей» соответственно.

8. Предложены механизмы, направленные на совершенствование нормы, предусматривающей ответственность за мошенничество в сфере компьютерной информации (далее – МСКИ), и некоторые механизмы противодействия такому мошенничеству:

– поскольку деяние, предусмотренное ст. 159.6 УК РФ, относится к преступлениям в сфере обращения цифровой информации и совершается с ее использованием, то указанную статью предлагается назвать «Мошенничество с использованием цифровой информации»;

– аргументировано, что мошенническое программное обеспечение относится к категории вредоносных цифровых программ. Уголовная ответственность за создание, использование и распространение мошеннического программного обеспечения (мошеннических программ) должна наступать по ст. 273 УК РФ;

– с целью дифференциации ответственности за мошенничество в сфере цифровой информации предлагается внести следующее дополнение в ч. 2 ст. 159.6 УК РФ: после слов *«значительного ущерба гражданину»* указать *«или с нарушением системы защиты цифровой информации»;*

– поскольку ИТКС «Интернет» содержит интернет-ресурсы, размещающие информацию о ВКП и программных средствах, предназначенных для нарушения систем защиты цифровой информации информационно-телекоммуникационных устройств, их систем и сетей, предлагается в порядке предупреждения этих преступлений ввести механизм внесудебного ограничения доступа на территории Российской Федерации к такой информации, дополнив п. 1 ч. 5 ст. 15.1 «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» следующим пунктом:

«ж) вредоносных программ и программных средств, предназначенных для нарушения систем защиты цифровой информации информационно-телекоммуникационных устройств, их систем и сетей».

9. Предложены механизмы, направленные на совершенствование норм уголовного законодательства за использование СТС НПИ, а также некоторые механизмы ограничения их оборота:

– предложено внести следующие изменения в наименование и диспозицию ст. 138.1 УК РФ: вместо слова *«предназначенных»* указать *«используемых»*;

– в примечании к ст. 138.1 УК РФ рекомендовано дать определение понятия «специальное техническое средство, используемое для негласного получения информации» в следующей редакции:

«Под специальным техническим средством, используемым для негласного получения информации, следует понимать программное либо аппаратное устройство, созданное или приспособленное исключительно для негласного перехвата, обработки и анализа информации»;

– поскольку в УК РФ недостаточно учтена общественная опасность неправомерного обращения со специальными техническими средствами (далее – СТС), используемыми для негласного получения информации, предложено установить в качестве квалифицирующего признака ответственность за применение таких средств в ч. 2 ст. 137 УК РФ, ч. 2 ст. 138 УК РФ, ч. 2 ст. 141 УК РФ и ч. 3 ст. 183 УК РФ;

– доказана целесообразность установления в ст. 226.1 УК РФ ответственности за контрабанду СТС, используемых для негласного получения информации, а также СТС, предназначенных для нарушения систем защиты цифровой информации, путем внесения следующих дополнений в наименование ст. 226.1 УК РФ и в диспозицию ч. 1 ст. 226.1 УК РФ: после слов *«ядерных материалов»* указать *«специальных технических средств, используемых для негласного получения информации, специальных технических средств, предназначенных для нарушения систем защиты цифровой информации»*;

– в целях государственного регулирования правоотношений, возникающих при обороте СТС, используемых для негласного получения информации, а также СТС, предназначенных для нарушения систем защиты цифровой информации и предупреждения соответствующих деяний, аргументировано предложение о принятии отдельного федерального закона «О специальных технических средствах». В нем необходимо определить правила их оборота, содержание используемых понятий, субъекты, которым разрешено использовать указанные

средства, установить порядок их применения, описать подробную классификацию указанных средств и т. д.

10. Поскольку преступные посягательства на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объектов имеют повышенную опасность, то с целью дифференциации уголовной ответственности предлагается:

– дополнить ст. 272 УК РФ частью пятой следующего содержания:

«5. Деяния, предусмотренные частями первой, второй, третьей и четвертой настоящей статьи, если они сопряжены с посягательством на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объектов, –

наказываются лишением свободы на срок до девяти лет».

– дополнить ст. 273 УК РФ частью четвертой следующего содержания:

«4. Деяния, предусмотренные частями первой, второй и третьей настоящей статьи, если они сопряжены с посягательством на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объектов, –

наказываются лишением свободы на срок до девяти лет».

В примечании 4 к ст. 272 УК РФ предлагаем дать определения понятий «критически важные объекты» и «потенциально опасные объекты» в следующей редакции:

«Под критически важными объектами в статьях 272 и 273 настоящего Кодекса понимаются объекты, нарушение (или прекращение) функционирования которых приводит к потере управления экономикой страны, субъекта или административно-территориальной единицы, ее необратимому негативному изменению (или разрушению) или существенному снижению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный период времени»;

«Под потенциально опасными в статьях 272 и 273 настоящего Кодекса объектами понимаются объекты, на которых используют, производят, перерабатывают, хранят, эксплуатируют, транспортируют или уничтожают радиоактивные, пожаровзрывоопасные и опасные химические и биологические вещества, а также гидротехнические сооружения, создающие реальную угрозу

возникновения источника кризисной ситуации».

11. Поскольку оборот СТС, предназначенных для нарушения систем защиты цифровой информации, имеет повышенную опасность, предложено:

– установить в качестве квалифицирующего признака ответственность за применение таких средств в ч. 3 ст. 272 УК РФ и в ч. 2 ст. 273 УК РФ;

– ввести отдельную норму об ответственности за незаконные производство, приобретение и (или) сбыт таких средств в следующей авторской редакции:

«Статья 273.1. Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации

1. Незаконные производство, приобретение и (или) сбыт специальных технических средств, предназначенных для нарушения систем защиты цифровой информации, –

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, 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 тот же срок.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, –

наказывается штрафом в размере от двухсот тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок».

12. Предлагается установить уголовную ответственность за приобретение или сбыт цифровой информации, заведомо добытой преступным путем, и дополнить УК РФ ст. 272.1 в следующей редакции:

«Статья 272.1. Приобретение или сбыт охраняемой законом цифровой информации, заведомо добытой преступным путем

1. Приобретение или сбыт охраняемой законом цифровой информации, заведомо добытой преступным путем, –

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, 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 тот же срок.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, –

наказывается штрафом в размере от двухсот тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок».

Теоретическая значимость диссертационного исследования состоит в том, что в нем впервые в теории уголовного права введено понятие «цифровая информация», комплексно освещаются понятие и виды преступлений в сфере обращения цифровой информации, а также обосновываются предложения по дополнению, совершенствованию и повышению эффективности уголовного законодательства об ответственности за данные преступления.

Результаты исследования могут послужить основой для дальнейших научных разработок по данной проблематике.

Практическая значимость диссертационного исследования заключается в том, что сформулированные в нем выводы, предложения и рекомендации могут быть применены в законотворческой деятельности по совершенствованию уголовного законодательства и иных нормативно-правовых актов; в правоприменительной деятельности при квалификации преступлений, посягающих на цифровую информацию; в процессе преподавания курсов уголовного и информационного права, правовых основ информационной безопасности и правовой защиты информации в юридических вузах и на курсах повышения квалификации судей, сотрудников правоохранительных органов и специалистов по защите информации; при подготовке учебников, учебных пособий и учебно-методических разработок по указанным дисциплинам.

Степень достоверности и апробация результатов диссертационного исследования. Диссертация выполнена на кафедре уголовного права и процесса Казанского инновационного университета имени В. Г. Тимирясова (ИЭУП), на которой проводилось ее рецензирование и обсуждение.

Степень достоверности результатов диссертационного исследования подкреплена результатами апробирования выводов, предложений и рекомендаций на практике и в учебном процессе, что подтверждается актами и справками внедрения.

Полученные результаты исследования были внедрены в учебный процесс юридического факультета Казанского инновационного университета имени В. Г. Тимирясова (ИЭУП), в правоприменительную деятельность отдела «К» Бюро специальных технических мероприятий и отдела по расследованию организованной преступной деятельности в кредитно-финансовых учреждениях и сфере компьютерной информации следственной части Главного следственного управления Министерства внутренних дел по Республике Татарстан, а также в практическую деятельность Центра специальной связи и информации Федеральной службы охраны Российской Федерации в Республике Татарстан.

Результаты проведенного исследования отражены в материалах международных и всероссийских научно-практических конференций. По теме диссертации соискателем подготовлено и опубликовано 40 научных работ, в том числе 17 статей в изданиях, рекомендованных ВАК при Минобрнауки России для опубликования основных научных результатов диссертации на соискание ученой степени кандидата наук. Общий объем опубликованных работ составляет 13,9 п. л.

В 2014 г. за цикл работ по вопросам ответственности за преступления в сфере обращения цифровой информации соискателю присуждена республиканская научная премия государственной поддержки молодых ученых Республики Татарстан (проект № 12-117т/П).

Структура диссертации определяется целями и задачами исследования. Диссертация состоит из введения, трех глав, включающих десять параграфов, заключения, списка сокращений и условных обозначений, списка литературы и восьми приложений.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы диссертационного исследования, рассматривается степень ее научной разработанности, определяются объект, предмет, цель и задачи научного исследования, характеризуется методологическая и теоретическая основы, эмпирическая и нормативно-правовая базы исследования, обосновывается научная новизна, формулируются основные положения, выносимые на защиту, теоретическая и практическая значимость, подтверждается достоверность результатов, приводятся данные об апробации результатов исследования и структуре диссертационной работы.

Первая глава **«Уголовно-правовая природа преступлений в сфере обращения цифровой информации»** состоит из двух параграфов.

В первом параграфе ***«Понятие цифровой информации»*** уточняется уголовно-правовая природа исследуемого феномена.

Соискателем проведен анализ определения компьютерной информации как предмета преступления. Рассмотрено толкование термина «цифровая информация» с трех позиций: филологической, технической и юридической. Определено, что понятие «цифровая информация» является родовым по отношению к понятиям «компьютерная информация» и «электронная информация». Синонимия таких понятий, как «цифровая», «компьютерная» и «электронная» информация, способна дезорганизовать правоприменительную деятельность.

С появлением современных беспроводных систем связи расширилась и сфера обращения информации. Поэтому в уточнении нуждается предмет преступления, предусмотренного ст. 272 УК РФ, – компьютерная информация, т. к. с технической точки зрения в современных информационно-телекоммуникационных устройствах, их системах и сетях обращается не компьютерная, а цифровая информация. Компьютерная информация является лишь подвидом цифровой информации. Поэтому в действующем уголовном законодательстве следует использовать более широкий по содержанию термин «цифровая информация», под которым следует понимать сведения (сообщения, данные), обращающиеся в информационно-телекоммуникационных устройствах, их системах и сетях.

Термин «цифровая информация» рекомендуем использовать в соответствующих статьях Особенной части УК РФ и отразить указанное понятие в ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Второй параграф ***«Понятие преступлений в сфере обращения цифровой информации»*** посвящен исследованию имеющихся подходов к определению рассматриваемого понятия в юридической науке, в частности соотношению понятий «преступление в сфере информационных технологий», «преступление в сфере высоких технологий», «компьютерное преступление», «киберпреступление».

Под преступлением в сфере обращения цифровой информации предлагается понимать предусмотренное уголовным законом виновно совершенное общественно опасное деяние, направленное на нарушение конфиденциальности, целостности, достоверности и доступности охраняемой законом цифровой информации.

Предлагаем относить к преступлениям в сфере обращения цифровой информации деяния, предусмотренные ст. 138.1, 159.6, 272, 273, 274 УК РФ.

Обосновано использование более широкого по содержанию термина «информационно-телекоммуникационные устройства, их системы и сети» в статьях Особенной части УК РФ вместо предусмотренного в ст. 274 УК РФ термина, указывающего на объекты обращения цифровой информации в виде «средств хранения, обработки или передачи компьютерной информации и ИТКС».

Поскольку ИТКС «Интернет» содержит интернет-ресурсы, размещающие информацию о способах совершения преступлений в сфере компьютерной информации, а также объявления о предоставлении незаконных услуг в этой сфере, предлагается в порядке предупреждения этих преступлений ввести механизм внесудебного ограничения доступа на территории Российской Федерации к такой информации.

Во второй главе **«Преступления в сфере компьютерной информации по уголовному кодексу Российской Федерации как виды преступлений в сфере обращения цифровой информации»,** состоящей из трех параграфов,

обосновываются и вносятся предложения по совершенствованию уголовной ответственности за указанные преступления.

В первом параграфе ***«Неправомерный доступ к компьютерной информации»*** отмечается несоответствие терминологии ст. 272 УК РФ современному состоянию науки и техники, рассматриваются негативные аспекты пробела уголовной ответственности за перехват охраняемой законом цифровой информации, и формулируется авторский вариант решения данной проблемы, обосновываются и предлагаются изменения и дополнения в ст. 272 УК РФ.

Основное отличие перехвата от неправомерного доступа, по мнению соискателя, заключается в том, что электромагнитному перехвату подвержена цифровая информация, циркулирующая в пространстве, а неправомерный доступ требует нарушения системы защиты информации информационно-телекоммуникационного устройства.

Установлено, что общественная опасность неправомерного доступа к цифровой информации близка по своей сути и общественной опасности перехвату цифровой информации в пространстве. Учитывая, что ст. 272 УК РФ не включает в себя указания на такое противоправное действие, как перехват цифровой информации, и в связи с вышесказанными пробелами предлагается установить ответственность за перехват охраняемой законом цифровой информации и внести соответствующие изменения в ст. 272 УК РФ.

В примечании к ст. 272 УК РФ предлагается дать определение понятия «перехват цифровой информации».

Во втором параграфе ***«Создание, использование и распространение вредоносных компьютерных программ»*** изучению подвергнута ст. 273 УК РФ. В результате анализа определены возможные направления совершенствования рассматриваемой нормы.

Выдвигается положение о том, что действие вредоносных компьютерных программ может нарушить работу средств защиты компьютерной информации. Законодатель, конечно же, хотел включить данные деяния в ст. 273 УК РФ, но почему-то связал это с нейтрализацией средств защиты компьютерной информации. Нам представляется, что слово «нейтрализация» является не совсем уместным, поскольку оно не является устоявшимся понятием в русском языке и не имеет единого смыслового значения.

В целях дифференциации уголовной ответственности предложено дополнить ст. 273 УК РФ частью четвертой, предусматривающей ответственность за деяния, предусмотренные частями первой, второй и третьей настоящей статьи, если они сопряжены с посягательством на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объектов.

В третьем параграфе ***«Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»*** изучается проблема установления уголовной ответственности за рассматриваемые нарушения.

Данная норма является бланкетной и отсылает к нормативно-правовым актам, устанавливающим требования к средствам хранения, обработки или передачи компьютерной информации. Видимо, к средствам хранения, обработки или передачи компьютерной информации относятся персональные компьютеры и иные информационно-телекоммуникационные устройства, в которых компьютерная информация обращается. Исходя из этого, было бы правильнее обобщить указанные средства хранения, обработки или передачи компьютерной информации и указать вместо них в названии и диспозиции ст. 274 УК РФ более широкие по содержанию «информационно-телекоммуникационные устройства, их системы и сети».

Основываясь на понятиях, используемых в законе, регулирующем отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, при применении информационных технологий, а также при обеспечении защиты информации, считаем такое решение оправданным.

Ввиду уточнения термина, указывающего на объекты обращения цифровой информации, обосновано предложение об изложении ст. 274 УК РФ в авторской редакции.

В третьей главе **«Иные виды преступлений в сфере обращения цифровой информации»**, состоящей из пяти параграфов, исследуются новые высокотехнологичные составы преступлений рассматриваемой тематики, в частности, МСКИ и незаконный оборот СТС НПИ. По результатам

проведенного анализа предложены пути усовершенствования положений УК РФ об ответственности за такие преступления и практики их применения.

Кроме того, в данной главе представлено решение задачи по разработке и обоснованию предложений об установлении уголовной ответственности за посягательства на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объектов; за незаконный оборот СТС, предназначенных для нарушения систем защиты цифровой информации; за приобретение или сбыт цифровой информации, заведомо добытой преступным путем.

В первом параграфе ***«Мошенничество в сфере компьютерной информации»*** изучению подвергнута ст. 159.6 УК РФ, предложены некоторые механизмы, направленные на совершенствование рассматриваемой нормы, и некоторые механизмы противодействия такому мошенничеству.

Доказано, что деяние, предусмотренное ст. 159.6 УК РФ, относится к преступлениям в сфере обращения цифровой информации и совершается с ее использованием. Указанную статью предложено назвать «Мошенничество с использованием цифровой информации».

Аргументировано, что мошенническое программное обеспечение относится к категории вредоносных цифровых программ. Уголовная ответственность за создание, использование и распространение мошеннического программного обеспечения (мошеннических программ) должна наступать по ст. 273 УК РФ.

Выявлено, что МСКИ может совершаться не только с использованием ВКП, но и с нарушением систем защиты цифровой информации. С целью дифференциации ответственности за мошенничество в сфере цифровой информации предложено внести в ч. 2 ст. 159.6 УК РФ указанное дополнение.

Поскольку ИТКС «Интернет» содержит интернет-ресурсы, размещающие информацию о ВКП и программных средствах, предназначенных для нарушения систем защиты цифровой информации информационно-телекоммуникационных устройств, их систем и сетей, предложено в порядке предупреждения этих преступлений ввести механизм внесудебного ограничения доступа на территории Российской Федерации к такой информации.

Во втором параграфе ***«Незаконный оборот специальных технических средств, предназначенных для негласного получения информации»*** изучению подвергнута ст. 138.1 УК РФ, предложены механизмы, направленные на совершенствование норм уголовного законодательства за использование СТС НПИ, а также некоторые механизмы ограничения их оборота.

Рекомендовано внести следующие изменения в наименование и диспозицию ст. 138.1 УК РФ: вместо слова «предназначенных» указать «используемых». Предложено в примечании к ст. 138.1 УК РФ раскрыть определение понятия «специальное техническое средство, используемое для негласного получения информации».

Доказано, что в УК РФ недостаточно учтена общественная опасность неправомерного обращения со СТС, используемыми для негласного получения информации, поскольку с их помощью могут быть получены сведения о частной жизни человека (ст. 137 УК РФ), нарушена тайна переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ), нарушена тайна голосования (ст. 141 УК РФ), получены сведения, составляющие коммерческую или банковскую тайну (ст. 183 УК РФ). В связи с этим предложено установить в качестве квалифицирующего признака ответственность за применение таких средств в ч. 2 ст. 137 УК РФ, ч. 2 ст. 138 УК РФ, ч. 2 ст. 141 УК РФ и ч. 3 ст. 183 УК РФ.

Доказана целесообразность установления в ст. 226.1 УК РФ ответственности за контрабанду СТС, используемых для негласного получения информации, а также СТС, предназначенных для нарушения систем защиты цифровой информации.

Аргументировано предложение о принятии отдельного федерального закона «О специальных технических средствах».

В третьем параграфе ***«Преступления, посягающие на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объектов»*** исследуется неправомерные воздействия на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объектов, обосновывается неоправданность применения понятия «кибертерроризм», предлагаются решения по дополнению ст. 272 и 273 УК РФ.

Думается, что разрушение информационной инфраструктуры критически важных и потенциально опасных объектов Российской Федерации путем неправомерного доступа к цифровой информации или внедрения в них ВКП может нанести значительный ущерб национальной безопасности, а также привести к экологической катастрофе, человеческим жертвам и иным тяжким последствиям.

Поскольку преступные посягательства на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объектов имеют повышенную опасность, то предложено ст. 272 и 273 УК РФ дополнить соответствующими частями, устанавливающими ответственность за совершение деяний, если они сопряжены с посягательством на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объектов. В предложенных частях статей УК РФ необходимо предусмотреть такие санкции, как лишение свободы на срок до девяти лет.

Кроме того, в примечании 4 к ст. 272 УК РФ предложено дать определения понятий «критически важные объекты» и «потенциально опасные объекты».

В четвертом параграфе ***«Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации»*** обосновывается и предлагается авторский вариант уголовно-правового ограничения обращения и применения таких предметов.

Современные информационно-телекоммуникационные устройства, системы и сети в основном хорошо защищены от атак на цифровую информацию, обращающуюся в них, так как находятся под охраной современных средств защиты цифровой информации. Этап проникновения в информационно-телекоммуникационные устройства с целью, например, копирования информации, наступает только после этапа обхода или нарушения системы защиты цифровой информации, предусмотренной в таких устройствах, иначе заполучить цифровую информацию преступнику просто не удастся.

Во многих случаях неправомерные деяния с цифровой информацией невозможны без использования СТС, предназначенных для нарушения систем защиты цифровой информации. Основное назначение таких СТС – это взлом или

обход имеющихся средств защиты цифровой информации в информационно-телекоммуникационных устройствах, их системах и сетях.

Поскольку оборот СТС, предназначенных для нарушения систем защиты цифровой информации, имеет повышенную опасность, предложено установить в качестве квалифицирующего признака ответственность за применение таких средств в ч. 3 ст. 272 УК РФ и в ч. 2 ст. 273 УК РФ, а также ввести отдельную норму об ответственности за незаконные производство, приобретение и (или) сбыт таких средств.

В пятом параграфе ***«Приобретение или сбыт цифровой информации, заведомо добытой преступным путем»*** предложено решение проблемы, связанной с отсутствием в УК РФ нормы, устанавливающей ответственность за приобретение или сбыт цифровой информации, заведомо добытой преступным путем.

Информацию обычно не признают имуществом, и поэтому манипуляции с ней не подпадают под признаки ст. 175 «Приобретение или сбыт имущества, заведомо добытого преступным путем» УК РФ, т. к. в названной норме под имуществом понимается совокупность вещей и материальных ценностей, находящихся во владении или законном пользовании физического или юридического лица. Думается, что цифровая информация имеет некоторую схожесть с другими вещами и материальными ценностями. Однако между ними имеется принципиальное различие: цифровую информацию, по сравнению, например, с драгоценным металлом или ценной бумагой, являющимися материальными ценностями, невозможно потрогать и ощутить, хотя носитель информации (например, Flash-карта), на котором находится цифровая информация, является материальной ценностью.

Учитывая, что ст. 175 «Приобретение или сбыт имущества, заведомо добытого преступным путем» УК РФ не содержит указаний на такой предмет, как цифровая информация, предложено установить уголовную ответственность за приобретение или сбыт цифровой информации, заведомо добытой преступным путем, и дополнить УК РФ ст. 272.1.

В **заключении** подводятся итоги диссертационного исследования, определяются основные направления оптимизации уголовного законодательства в сфере обращения цифровой информации и определяются перспективы дальней-

ших направлений исследования.

В **приложениях** приведена анкета экспертного опроса с таблицей и диаграммой ее результатов, сведения о зарегистрированных в Российской Федерации преступлениях в сфере компьютерной информации, а также сведения о зарегистрированных в Российской Федерации преступлениях, предусмотренных ст. 159.6, 272, 273, 274 УК РФ.

Основные научные результаты диссертационного исследования опубликованы в следующих **работах:**

I. Работы, опубликованные в изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве образования и науки Российской Федерации:

1. *Бегишев, И. Р.* О некоторых способах совершения противоправных деяний в современных информационно-телекоммуникационных системах обращения цифровой информации / И. Р. Бегишев // Информация и безопасность. – 2009. – № 4. – С. 607–610 (0,45 п. л.).

2. *Бегишев, И. Р.* Уголовная ответственность за приобретение или сбыт цифровой и документированной информации, заведомо добытой преступным путем / И. Р. Бегишев // Актуальные проблемы экономики и права. – 2010. – № 1. – С. 123–126 (0,5 п. л.).

3. *Бегишев, И. Р.* Проблемы противодействия преступным посягательствам на информационные системы критически важных и потенциально опасных объектов / И. Р. Бегишев // Информационная безопасность регионов. – 2010. – № 1. – С. 9–13 (0,55 п. л.).

4. *Бегишев, И. Р.* Проблемы ответственности за незаконные действия с информацией, заведомо добытой преступным путем / И. Р. Бегишев // Безопасность информационных технологий. – 2010. – № 1. – С. 43–44 (0,25 п. л.).

5. *Бегишев, И. Р.* Преступления в сфере обращения цифровой информации: состояние, пробелы и пути их решения / И. Р. Бегишев // Информационное право. – 2010. – № 2. – С. 18–21 (0,4 п. л.).

6. *Бегишев, И. Р.* Изготовление, сбыт и приобретение специальных технических средств, предназначенных для нарушения систем защиты цифровой информации: правовой аспект / И. Р. Бегишев // Информация и безопасность. – 2010. – № 2. – С. 255–258 (0,45 п. л.).

7. *Бегишев, И. Р.* Информационное оружие как средство совершения преступлений / И. Р. Бегишев // Информационное право. – 2010. – № 4. – С. 23–25 (0,3 п. л.).

8. *Бегишев, И. Р.* Современное состояние преступлений в сфере обращения цифровой информации / И. Р. Бегишев // Информация и безопасность. – 2010. – № 4. – С. 567–572 (0,7 п. л.).

9. *Бегишев, И. Р.* Проблемы уголовной ответственности за обращение со специальными техническими средствами, предназначенными для негласного получения информации / И. Р. Бегишев // Следователь. – 2010. – № 5. – С. 2–4 (0,35 п. л.).

10. *Бегишев, И. Р.* Уголовно-правовые аспекты кибертерроризма / И. Р. Бегишев // Правовые вопросы национальной безопасности. – 2010. – № 5–6. – С. 34–37 (0,45 п. л.).

11. *Бегишев, И. Р.* Ответственность за нарушение работы информационно-телекоммуникационных устройств, их систем и сетей / И. Р. Бегишев // Безопасность информационных технологий. – 2011. – № 1. – С. 73–75 (0,35 п. л.).

12. *Бегишев, И. Р.* Перехват охраняемой законом цифровой информации: уголовно-правовые аспекты / И. Р. Бегишев // Информационная безопасность регионов. – 2011. – № 1. – С. 78–81 (0,45 п. л.).

13. *Бегишев, И. Р.* Цифровая информация: понятие и сущность как предмета преступления по российскому уголовному праву / И. Р. Бегишев // Академический юридический журнал. – 2011. – № 2. – С. 47–55 (1,1 п. л.).

14. *Бегишев, И. Р.* Меры предупреждения преступлений в сфере обращения цифровой информации / И. Р. Бегишев // Информация и безопасность. – 2011. – № 3. – С. 433–438 (0,75 п. л.).

15. *Бегишев, И. Р.* Правовые аспекты безопасности информационного общества / И. Р. Бегишев // Информационное общество. – 2011. – № 4. – С. 54–59 (0,5 п. л.).

16. *Бегишев, И. Р.* Создание, использование и распространение вредоносных компьютерных программ / И. Р. Бегишев // Проблемы права. – 2012. – № 3. – С. 218–221 (0,35 п. л.).

17. *Бегишев, И. Р.* Некоторые вопросы противодействия мошенничеству

в сфере компьютерной информации / И. Р. Бегишев // Вестник Казанского юридического института МВД России. – 2016. – № 3. – С. 112–117 (0,6 п. л.).

II. Работы, опубликованные в иных изданиях:

18. *Бегишев, И. Р.* Уголовная ответственность за перехват цифровой информации / И. Р. Бегишев // Information Security / Информационная безопасность. – 2010. – № 4. – С. 16–17 (0,2 п. л.).

19. *Бегишев, И. Р.* Информационные войны: предупреждение и предотвращение угроз / И. Р. Бегишев // Защита информации. Inside. – 2010. – № 4. – С. 34–35 (0,2 п. л.).

20. *Бегишев, И. Р.* Уголовная ответственность за нарушение работы цифровых устройств, их систем и сетей / И. Р. Бегишев // Information Security / Информационная безопасность. – 2010. – № 5. – С. 22–23 (0,2 п. л.).

21. *Бегишев, И. Р.* Уголовно-правовое нововведение в сфере защиты цифровой информации / И. Р. Бегишев // Information Security / Информационная безопасность. – 2011. – № 1. – С. 18–19 (0,2 п. л.).

22. *Бегишев, И. Р.* Противодействие утечкам цифровой информации: вопросы уголовной ответственности / И. Р. Бегишев // Защита информации. Inside. – 2011. – № 2. – С. 32–34 (0,35 п. л.).

23. *Бегишев, И. Р.* Открытое ПО: вопросы права, безопасности и последствий / И. Р. Бегишев // Information Security / Информационная безопасность. – 2011. – № 4. – С. 28–29 (0,2 п. л.).

24. *Бегишев, И. Р.* Новое в ответственности за неправомерный доступ к компьютерной информации по Уголовному кодексу Российской Федерации / И. Р. Бегишев // Правосудие в Татарстане. – 2011. – № 4. – С. 42–44 (0,35 п. л.).

25. *Бегишев, И. Р.* Новеллы в уголовном законодательстве об ответственности за преступления в сфере компьютерной информации / И. Р. Бегишев // Information Security / Информационная безопасность. – 2012. – № 2. – С. 52–53 (0,2 п. л.).

26. *Бегишев, И. Р.* Преступления в сфере обращения цифровой информации. Результаты научного исследования / И. Р. Бегишев // Information Security / Информационная безопасность. – 2012. – № 6. – С. 8–10 (0,35 п. л.).

27. *Бегишев, И. Р.* Ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и инфор-

мационно-телекоммуникационных сетей / И. Р. Бегишев // Вестник УрФО. Безопасность в информационной сфере. – 2012. – № 1. – С. 15–18 (0,3 п. л.).

28. *Бегишев, И. Р.* Новый взгляд на мошенничество в сфере компьютерной информации / И. Р. Бегишев // Information Security / Информационная безопасность. – 2016. – № 1. – С. 28–29 (0,2 п. л.).

III. Статьи, тезисы докладов и сообщений на научных конференциях:

29. *Бегишев, И. Р.* Уголовная ответственность за преступления в сфере систем мобильной связи / И. Р. Бегишев // Правовая система и вызовы современности: материалы Международной науч. конф. студентов, аспирантов и молодых ученых. Ч. 2. – Уфа: РИЦ БашГУ, 2006. – С. 214–216 (0,15 п. л.).

30. *Бегишев, И. Р.* Защита информации в сфере предпринимательской деятельности в системе мобильной связи / И. Р. Бегишев // Предпринимательство и его место в экономике современной России: материалы науч.-практ. конф. – М.: Издательский дом «Юриспруденция», 2006. – С. 42–45 (0,2 п. л.).

31. *Бегишев, И. Р.* О соответствии терминологии статьи 272 УК РФ современному состоянию науки и техники / И. Р. Бегишев // Актуальные проблемы юридической науки и правоприменительной практики: сб. науч. трудов (по материалам VIII Международной заочной науч.-практ. конф., 6 ноября 2009 г.). В 2 ч. Ч. 1 – Киров, 2009. – С. 37–40 (0,25 п. л.).

32. *Бегишев, И. Р.* К вопросу о совершенствовании уголовной ответственности за неправомерный доступ к компьютерной информации / И. Р. Бегишев // Казанские научные чтения студентов и аспирантов – 2009: материалы докладов Всероссийской науч.-практ. конф. студентов и аспирантов, 25 декабря 2009 г. В 2 т. Т. 2. – Казань: Изд-во «Познание» Института экономики, управления и права, 2010. – С. 42–43 (0,1 п. л.).

33. *Бегишев, И. Р.* О понятии цифровой информации: уголовно-правовой аспект / И. Р. Бегишев // Актуальные проблемы права на современном этапе развития российской государственности: материалы Всероссийской науч.-практ. конф., 25–26 марта 2010 г. В 3 ч. Ч. 2. – Уфа: РИЦ БашГУ, 2010. – С. 67–71 (0,25 п. л.).

34. *Бегишев, И. Р.* Специальные технические средства в уголовном праве / И. Р. Бегишев // «Норма. Закон. Законодательство. Право». Сб. тезисов 12-й

Всероссийской науч. конф. студентов и аспирантов, 22–24 апреля 2010 г. – Пермь, 2010. – С. 159–160 (0,1 п. л.).

35. *Бегишев И. Р.* Ответственность за незаконное производство, сбыт или приобретение специальных технических средств, предназначенных для разрушения систем зашиты информации / И. Р. Бегишев // Эволюция государственно–правовых систем современности: сб. статей Всероссийской науч.-практ. конф., 20 февраля 2010 г. – Абакан, 2010. – С. 194–195 (0,5 п. л.).

36. *Бегишев, И. Р.* Уголовная ответственность за перехват и сбыт цифровой информации: пробелы и пути их решения / И. Р. Бегишев // Актуальные проблемы права России и стран СНГ – 2010: материалы XII Международной науч.-практ. конф. с элементами научной школы, 1–2 апреля 2010 г. – Челябинск, 2010. – С. 117–120 (0,35 п. л.).

37. *Бегишев, И. Р.* Уголовно-правовая охрана информационной инфраструктуры критически важных и потенциально опасных объектов Российской Федерации / И. Р. Бегишев // Россия – правовое государство: проблемы и пути формирования: материалы Всероссийской науч.-практ. конф., 4 марта 2010 г. – Дербент, 2010. – С. 116–119 (0,25 п. л.).

38. *Бегишев, И. Р.* Уголовная ответственность за незаконное обращение специальных технических средств, предназначенных для нарушения систем защиты информации / И. Р. Бегишев // Актуальные вопросы и проблемы применения уголовного законодательства: материалы Всероссийской заочной науч.-практ. конф., 1 апреля 2010 г. – Уфа: РИЦ БашГУ, 2010. – С. 12–15 (0,2 п. л.).

39. *Бегишев, И. Р.* О криминализации незаконного ознакомления с охраняемой законом цифровой информацией / И. Р. Бегишев // Уголовное право в эволюционирующем обществе: проблемы и перспективы: сб. науч. ст. по материалам Международной науч.-практ. конф., 24 мая 2010 г. / ред. кол.: А. А. Гребеньков (отв. ред.) [и др.]; Юго-Зап. гос. ун-т. – Курск, 2010. – С. 139–141 (0,15 п. л.).

40. *Бегишев, И. Р.* Программное обеспечение с открытыми исходными кодами: нормативно-правовое регулирование / И. Р. Бегишев // XIX Туполевские чтения: Международная молодежная науч. конф., 24–26 мая 2011 г.: материалы конф. Т. 5. Казань: Изд-во Казан. гос. техн. ун-та. 2011. – С. 488–490 (0,15 п. л.).

Подписано в печать 3 июля 2017 г.
Формат бумаги 60х90/16. Гарнитура Times NR.
Тираж 150 экз. Усл. п. л. 1,5. Заказ № 91.
Отпечатано с готового оригинал-макета в типографии
Казанского инновационного университета имени В. Г. Тимирясова (ИЭУП).
420108, г. Казань, ул. Зайцева, д. 17.
Тел.: (843) 231-92-90. Факс: (843) 292-61-59.
E-mail: info@ieml.ru