На правах рукописи

Федеральное государственное автономное образовательное учреждение высшего образования Казанский (Приволжский) федеральный университет

Гайфутдинов Рамиль Рустамович

ПОНЯТИЕ И КВАЛИФИКАЦИЯ ПРЕСТУПЛЕНИЙ ПРОТИВ БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

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

Диссертация на соискание ученой степени кандидата юридических наук

Научный руководитель:
доктор юридических наук, профессор
М. В. Талан

Казань – 2017

Оглавление

Введение

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.

Указом Президента Российской Федерации 5 декабря 2016 года утверждена новая Доктрина информационной безопасности Российской Федерации[1]. Она основана на Стратегии национальной безопасности Российской Федерации от 31 декабря 2015 г. и развивает ее соответствующие положения[2].

Повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям является важной составляющей обеспечения информационной безопасности. Вместе с тем требование законности в информационной сфере и правовое равенство всех их участников основываются на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом и представляют собой один из принципов деятельности государственных органов по обеспечению ее безопасности.

В Стратегии развития информационного общества в Российской Федерации на 2017-2030 гг. подчеркивается, что обеспечение национальных интересов в области цифровой экономики является одним из приоритетов при развитии информационного общества[3]. Этот вектор развития актуализирует Стратегию научно-технологического развития Российской Федерации, в которой среди иных

---

[1] Доктрина информационной безопасности Российской Федерации : утв. Указом Президента РФ от 5 дек. 2016 г. № 646 // Собр. законодательства Рос. Федерации. 2016. № 50, ст. 7074.

[2] Стратегия национальной безопасности Российской Федерации : утв. Указом Президента РФ от 31 дек. 2015 г. № 683 // Собр. законодательства Рос. Федерации. 2016. № 1 (часть II), ст. 212.

[3] Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы : утв. Указом Президента РФ от 9 мая 2017 г. № 203 // Собр. законодательства Рос. Федерации. 2017. № 20, ст. 2901.

приоритетных направлений указываются те, которые обеспечивают переход к цифровым, интеллектуальным производственным технологиям, роботизированным системам, новым материалам и способам конструирования, созданию систем обработки больших объемов данных, машинного обучения и искусственного интеллекта, в том числе противодействие киберугрозам для общества, экономики и государства[4].

Иными словами, 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 негативное воздействие на национальную безопасность в целом, развитие науки и техники, а также цифровой экономики в Российской Федерации.

Уголовный кодекс Российской Федерации (далее – УК РФ) предусматривает достаточно строгие меры уголовно-правовой ответственности за совершение различных видов преступлений против безопасности компьютерной информации (ст.ст. 272-274 УК РФ).

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.[5] и в полной мере согласуется с положениями Доктрины (п. 22) о защите информационной инфраструктуры как одной из стратегических целей обеспечения информационной безопасности.

Анализ статистических данных о преступлениях против безопасности компьютерной информации (ст.ст. 272-274 УК РФ) убеждает в том, что криминальная активность отражается в них не в полной мере. Так, за 2010-2016

---

[4] О научно-технологическом развитии Российской Федерации : утв. Указом Президента РФ от 1 дек. 2016 г. № 642 // Собр. законодательства Рос. Федерации. 2016 г. № 49, ст. 6887.

[5] 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).

гг. в Российской Федерации число осужденных за рассматриваемые преступления составляло соответственно 321, 258, 280, 268, 218, 235 и 185 человек. Однако существующий уровень латентности указанной преступности подтверждается криминологическими исследованиями. Сходные тенденции характерны не только для нашей страны. Согласно экспертным данным, в мире ежегодно наблюдается рост компьютерной преступности и производного от них размера ущерба[6].

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, соответствующих изменений в общественных отношениях, 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),

[6] 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).

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 применительно 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. 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 в данном деле. Это позволяет говорить о квалификации преступления в узком и широком смысле. Понимание квалификации преступления только как содержащуюся в уголовно-процессуальном акте ссылку на пункт, часть и статью УК РФ имеет теоретическое и законодательное основание.

2. Будучи одной из *форм* (*разновидностей*) уголовно-правовой квалификации квалификация преступления может оказаться одновременно ее следующим *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, 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.

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 которым 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 процесс обеспечения информационной безопасности, одной из целей и результатом которых является «безопасность информации». Таким образом, информационная безопасность представляет собой требуемое состояние объекта, которое достигается посредством урегулированного правом защиты информации.

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

Безопасность обращения компьютерной информации – это отсутствие причинения вреда или ее 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 опасность

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 ст. 272 УК РФ, следует признавать безопасность охраняемой законом компьютерной информации, которая обеспечивается правомерным доступом к ней, ст. 273 УК РФ – безопасность компьютерной информации и средств защиты компьютерной информации, обеспечиваемая правомерным оборотом компьютерных программ и компьютерной информации, 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, 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. Указанный первый вид вредоносной компьютерной программы либо иной компьютерной компьютерной информации подобного рода является более широким определением по сравнению с ее вторым видом, 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 времени 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 следует признать, 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 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 информации 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 проведения 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 подход 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 проводилось 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).

Глава 1. Основные положения теории квалификации преступления и их интерпретация к уголовно-правовой оценке деяний против безопасности компьютерной информации

§ 1. Понятие квалификации преступления, ее виды, содержание и правовые основы

Термин «квалификация» [7] определяется обычно как «характеристика предмета явления, отношение его к какой-либо категории, группе» [8]. В этом качестве он обычно используется в юриспруденции. К определению квалификации *преступления* в уголовно-правовой литературе существуют разные подходы [9]. Однако в основе многих современных дефиниций лежит определение, предложенное в свое время академиком В. Н. Кудрявцевым. Он сформулировал его как «установление и юридическое закрепление точного соответствия между фактическими признаками совершенного деяния и признаками состава преступления, предусмотренного уголовным законом» [10]. Сущность рассматриваемого нами термина достаточно точно определяет характер и содержание этой деятельности: квалификатор выявляет конкретные признаки деяния, сопоставляет их с законодательным описанием преступления, а свой вывод закрепляет в виде решения, изложенного в определенном уголовно-процессуальном акте. Поэтому данное определение представляет собой основу для характеристики этого вида *правоприменения*, а также для определения квалификации преступления как универсального понятия.

Преимущество концепции, выдвинутой академиком В. Н. Кудрявцевым, заключается, во-первых, в том, что квалификация рассматривается одновременно как процесс и как его результат. Ученый раскрывает содержание этого процесса через термин «установление», который становится признаком определения, посредством которого акцентируется, в первую очередь, *деятельная* сторона

---

[7] От латинских слов quails – какого качества и facere – делать.
[8] Словарь иностранных слов. М.: Русский язык, 1988. С. 223.
[9] См., напр.: Герцензон А. А. Квалификация преступления. М.: Изд-во ВЮА КА, 1947. С. 4; Левицкий Г. А. Квалификация преступления (общие вопросы) // Правоведение, 1962. № 1. С. 144.
[10] Кудрявцев В. Н. Теоретические основы квалификации преступлений // М.: Госюриздат, 1963. С. 8.

квалификации: а) выявление конкретных признаков деяния и определение признаков соответствующего состава преступления, б) их сопоставление друг с другом. Вывод о точном соответствии сопоставляемых объектов исследования имеет характер решения.

Между тем, следует отметить, что содержащийся в анализируемом определении признак «юридическое закрепление» не свойственен любому виду квалификации преступления, т.е. не является универсальным: квалификацию преступлений осуществляют не только уполномоченные государством субъекты, но и иные лица, в том числе не имеющие отношения к юриспруденции как профессии. Не случайно квалификацию обычно подразделяют на официальную и неофициальную. Юридическое закрепление вывода производится в соответствующем правоприменительном акте, принимаемым уполномоченными на то органами и лицами[11]. Таким образом, эта составляющая рассматриваемого определения присуща только для характеристики официальной (иногда ее именуют легальной) квалификации преступления. При неофициальной ее разновидности вывод о совпадении (тождестве) также может быть зафиксирован в устной или письменной формах, но не в официальном (уголовно-процессуальном) документе или форме. Неофициальная квалификация может быть доктринальной, профессиональной, обыденной.

При характеристике квалификации преступления следует учитывать, что в основе ее понимания, ее ядром является уголовно-правовая оценка. Некоторые ученые считают ее родовым признаком определяемого понятия[12]. Однако Р. А. Сабитов прав, полагая, что «уголовно-правовую оценку» можно употребить при определении ряда общих понятий[13]. Квалификация преступления есть одна из разновидностей *уголовно-правовой оценки* явления, опирающейся на уголовный закон (или представления о его содержании)[14].

---

[11] См., напр.: ст.ст. 171, 220, 225, 226[7] УПК РФ.

[12] См., напр.: Никонов В. А. Основы теории квалификации преступлений (алгоритмический подход): учебное пособие. Тюмень: Изд-во Тюмен. Ун-та, 2001. С. 24.

[13] См.: Сабитов Р. А. Теория и практика уголовно-правовой квалификации. М.: Юрлитинформ, 2013. С. 27.

[14] См.: Гаухман Л. Д. Квалификация преступлений: закон, теория, практика. 3-е изд., перераб. и дополн. М.: АО «Центр ЮрИнфоР», 2005. С. 6.

При характеристике определения квалификации преступления, ставшего традиционным, общепринятым, обычно обращается внимание на то, что термин (и признак) «установление» несет в определении только *процессуальную* (деятельную) нагрузку, а его *результативный* аспект обозначается через *закрепление* вывода в соответствующем правоприменительном акте. Думается, что в определении квалификации указанный термин (и признак) заключает в себя смысловую нагрузку, сочетающую деятельный и результативный аспекты. Этот подход позволяет выработать общее определение квалификации преступления, пригодное для характеристики как официальной, так и неофициальной ее разновидностей.

С этимологической точки зрения «установить» означает не только доказать, выяснить, но и *обнаружить* [15] . Следовательно, любой вид квалификации преступления можно рассматривать в качестве *установления* точного соответствия между признаками совершенного деяния и признаками состава преступления, включая вывод об этом соответствии. Признак «юридическое закрепление» следует полагать дополнительным, ибо он присущ только официальному виду квалификации как разновидности правоприменительной деятельности. Вывод о соответствии сопоставленных объектов при неофициальной квалификации всегда имеет место как некое решение, но официальных последствий за собой не влечет.

В уголовно-правовой литературе нередко объектами сопоставительного исследования при квалификации преступления называются фактические признаки содеянного и признаки состава преступления. Такой подход нельзя признать оправданным с методологической (философской) точки зрения. Установить тождество или хотя бы точное соответствие между фактическими признаками деяния и уголовно-правовыми признаками состава преступления затруднительно или невозможно без предварительной деятельности по *извлечению* из фактической основы (фактических данных) юридически значимых признаков. Это деятельность по преобразованию социальных фактов в сопоставимый (юридический) вид.

---

[15] Толковый словарь русского языка под ред. С.И. Ожегова и Н.Ю. Шведовой. М., 1997. URL: http://dic.academic.ru/dic.nsf/ogegova/253790 (дата обращения 17.07.17).

Признавая необходимость этой логико-юридической операции, некоторые ученые не включают ее в содержание квалификации преступления, полагая, что это предпосылка квалификации, деятельность, предшествующая ей[16]. Таким образом, официальная квалификация преступления представляет собой установление тождества между юридически значимыми признаками совершенного деяния и признаками определенного состава преступления, предусмотренного уголовным законом и иными его положениями, с последующей его фиксацией в установленной уголовно-процессуальной форме.

В литературе также выделяют и иные виды квалификации по иным основаниям: правильную и неправильную; предварительную и окончательную; адекватную, избыточную и неполную[17].

Содержание официальной квалификации преступления в процессуальном отношении представляет некоторую совокупность логико-юридических операций и соответствующих уголовно-правовых оценок, осуществляемых правоприменителем при окончательной уголовно-правовой оценке совершенного уголовно-наказуемого как определенного вида преступления деяния. В теории уголовного права их иногда именуют *этапами* квалификации преступления, причем нередко их связывают со стадиями уголовного процесса[18]. Мы разделяем точку зрения А. И. Рарога, который полагает, что содержание квалификации преступления следует отличать от таких стадий, поскольку на каждой процессуальной стадии при квалификации преступления осуществляются одни и те же логико-юридические операции[19].

---

[16] См.: Сабитов Р. А. Указ. соч. С. 27.

[17] О видах квалификации преступлений см. подробнее.: Сабитов Р. А. Указ. соч. С. 31; Гаухман Л. Д. Указ. соч. С. 19-23; Дуюнов В. К., Хлебушкин А. Г. Квалификация преступлений: законодательство, теория, судебная практика: Монография. М.: РИОР: ИНФРА-М, 2012. С. 7; Корнеева А. В. Теоретические основы квалификации преступлений : учеб. Пособие / под. ред. А. И. Рарога. М. : ТК Велби, Изд-во Проспект, 2007. С. 6.

[18] См.: Кудрявцев В. Н. Общая теория квалификации преступлений. М., 1999. С. 13-14; Кузнецова Н. Ф. Проблемы квалификации преступлений : лекции по спецкурсу «Основы квалификации преступлений» / науч. ред. и предисл. академика В. Н. Кудрявцева. М.: Изд. Дом Городец, 2007. С. 56, 58; Семернева Н. К. Квалификация преступлений (части Общая и Особенная): научно-практическое пособие. М.: Проспект; Екатеринбург: УрГЮА, 2014. С. 15 и др.

[19] См.: Рарог А. И. Квалификация преступлений по субъективным признакам. С.-Пб.: Юрид. центр Пресс, 2002. С. 24.

В литературе предлагаются иные подходы к этапизации процесса квалификации преступления[20]. Они имеют много общего, хотя и различаются по отдельным составляющим. Достаточно полно и убедительно процесс квалификации преступления как совокупность следующих одна за другой логико-юридических операций представлена И. А. Тархановым[21].

Первый этап квалификации преступления заключается в *извлечении* из совокупности фактических доказанных по делу юридически-значимых (уголовно-правовых) признаков. Это позволяет привести фабулу дела в юридический вид [22] . Только в этом случае можно разрешить проблему установления искомого тождества (точного соответствия). Некоторые специалисты считают, что первоначальным этапом квалификации преступления является *установление* фактических обстоятельств дела. Однако, как вполне справедливо полагал В. Н. Кудрявцев, такая деятельность является лишь предпосылкой правильного применения нормы права[23]. В уголовном процессе она именуется доказыванием. В этом смысле квалификация преступления есть уголовно-правовая *оценка* доказанных фактов.

На следующем этапе создается уголовно-правовая база как предназначенная юридическая основа для будущего сопоставления выявленных юридически-значимых признаков деяния с признаками составов преступления, претендующих на применение. Она представляет собой, таким образом, некоторую совокупность составов преступлений. Уголовно-правовая база формируется путем выдвижения *квалификационных* версий как юридических гипотез.

На следующем этапе осуществляется логико-юридическая операция *сопоставления* юридических значимых признаков деяния с признаками тех составов преступлений (и некоторых норм Общей части УК), которые включены в уголовно-правовую базу. Иными словами, осуществляются а) установление

---

[20] См., напр.: Корнеева А. В. Указ. соч. С. 12; Кузнецова Н. Ф. Указ. соч. С. 58; Гаухман Л. Д. Указ. соч. С. 317-318; Дуюнов В. К., Хлебушкин А. Г. Указ. соч. С. 9; Сабитов Р. А. Указ. соч. С. 46-47.

[21] Тарханов И. А. Юридическая квалификация: понятие и место в правоприменительном процесс // Российский юридический журнал. Екатеринбург: Изд-во УрГЮА, 2012. № 3 (84). С. 134-138.

[22] В структуре обвинения в материально-правовом смысле они именуются юридической формулировкой.

[23] Кудрявцев В. Н. Теоретические основы квалификации преступлений // М.: Госюриздат. 1963. С. 14.

наличия или отсутствия точного соответствия между юридически значимыми признаками деяния и соответствующими объективными и субъективными признаками отдельных составов преступлений, б) процесс исключения тех или иных составов из сформированной ранее уголовно-правовой базы.

В результате такого сопоставления делается *вывод* о полном соответствии (тождестве) юридически значимых признаков признакам определенного состава (или составам – при множественности преступлений) преступления. Он завершает процедуру установления точного соответствия (тождества) сопоставляемых объектов исследования.

Как отмечалось ранее, способ фиксации сформулированного в определенном виде вывода связан с особенностями субъекта квалификации. При официальной квалификации преступления вывод о тождестве фиксируется в процессуальном акте, установленном Уголовно-процессуальном кодексом Российской Федерации (далее – УПК РФ), например, в обвинительном заключении, акте.

В теории права существует дискуссия по вопросу о юридической (правовой) природе квалификации преступления. По мнению большинства ученых, это уголовно-правовая категория. Однако высказывается идея о том, что это комплексное явление, имеющее уголовно-правовую и уголовно-процессуальную природу, поскольку официальная квалификация получает отражение в соответствующей уголовно-процессуальной форме. Этот концептуальный взгляд содержит некоторое рациональное зерно, поскольку правовая квалификация является структурным элементом обвинения в материальном правовом смысле и фиксируется, как уже отмечалось, в определенной форме. Анализируемое позволяет также рассмотреть вопрос о квалификации преступления в несколько ином, более широком контексте. В теории уголовного права фактически сложилось понимание квалификации преступления в широком и узком смыслах, поскольку иногда такую квалификацию определяют как ссылку на статью (ее часть или пункт) УК РФ.

Составными элементами обвинения признаются фабула дела, юридическая формулировка и правовая квалификация [24]. Юридическая формулировка и правовая квалификация имеют много общего, но и отличаются друг от друга. Строго говоря, и юридическая формулировка, и правовая квалификация – есть *уголовно-правовая оценка содеянного*, но излагаемая в разной форме. Это позволяет говорит о квалификации преступления в широком ее понимании.

Так, обвинение по одному из изученных дел выглядит следующим образом: Д. признан виновным в подстрекательстве, то есть склонении другого лица путем уговора на совершение неправомерного доступа к охраняемой законом компьютерной информации с использованием своего служебного положения, повлекшего копирование компьютерной информации [25]. Таким образом, юридическая формулировка представляет собой только описание всех признаков содеянного, закрепленных в уголовно-правовой норме[26].

Правовая квалификация преступления, понимаемая как ссылка на статью УК РФ, определяется юридической формулировкой, однако может не совпадать с ней полностью. По вышеуказанному делу квалификация преступления выразилась в ссылке на ч. 4 ст. 33, ч. 3 ст. 272 УК РФ, т.е. при ссылке на УК получили отражение все признаки, указанные в юридической формулировке. Однако иногда при квалификации преступления в ее узком значении такого совпадения может и не быть, ибо, по правилам такой квалификации, в случаях наличия в деянии нескольких квалифицирующих признаков, один из которых является особо квалифицирующим, делается ссылка только на последний из них.

Проблема *основ* квалификации преступлений имеет несколько аспектов: методологические, логические и юридические. Поэтому в литературе выделяют философские (методологические), логические, психологические, *правовые (нормативные, юридические)* основы квалификации преступлений[27]. При этом

---

[24] См.: Фаткуллин Ф. Н. Изменение обвинения. М.: Юридическая литература, 1971. С. 22-23.

[25] Апелляционное определение Самарского областного суда от 16.01.17 г. по делу № 22-190/2017 // ГАС «Правосудие». URL: http://oblsud.sam.sudrf.ru/ (дата обращения: 13.07.17)

[26] без ссылки на статью (часть, пункт) УК РФ.

[27] См.: Дуюнов В. К., Хлебушкин А. Г. Указ. соч. С. 7-9; Уголовное право России. Особенная часть: Учебник / Под ред. Ф. Р. Сундурова, М. В. Талан. М.: Статут, 2012. С. 20. (автор главы Л. Л. Кругликов).

философскими основами обычно считаются категории общего, особенного и единичного (отдельного), сущность и явление, содержание и форма. А. В. Наумов и А. С. Новиченко рассматривают квалификацию как «логический процесс перехода от исходного знания к выводному через обосновывающее знание»[28]. По мнению Р. А. Сабитова, юридическими *основами* квалификации преступления следует считать совокупность норм, которые *используются* правоприменителем для уголовно-правовой оценки деяний, а ее *основанием* – состав преступления[29]. Таким образом, в теории предпринимается попытка разграничить понятия «основы» и «основания» квалификации преступления. В зависимости от этого выделять круг источников, на который опирается правоприменитель при квалификации преступления.

В качестве правовой (юридической) основы квалификации преступления иногда предлагается считать либо уголовный *закон* (УК РФ), либо уголовно-правовую *норму*, или *состав* преступления, признаки которого содержатся в УК РФ[30]. Обосновывается такая позиция обычно тем, что для закрепления результата квалификации преступления имеют значение ссылки на пункт, часть и статью состава преступления, а в некоторых случаях – и на нормы Общей его части. Каждая из названных точек зрения имеет рациональное зерно.

Действительно, именно уголовный закон является правовой основой для квалификации преступления, поскольку в нем содержатся уголовно-правовые нормы, в которых, в свою очередь, излагается описание признаков соответствующих составов преступления как законодательных моделей для квалификации преступлений[31]. Кроме того, содержащий ряд нормативных правил квалификации преступления, предписания необходимые для квалификации преступлений при особых формах преступной деятельности (неоконченная преступная деятельность, соучастие в преступлении, их множественность и

---

[28] См.: Наумов А. В., Новиченко А. С. Законы логики при квалификации преступлений. М.: Юридическая литература, 1978. С. 76.
[29] См.: Сабитов Р. А. Указ. соч. С. 107.
[30] См.: Дуюнов В. К., Хлебушкин А. Г. Там же.
[31] См.: Тарханов И. А. Юридическая квалификация: понятие и место в правоприменительном процесс // Российский юридический журнал. Екатеринбург: Изд-во УрГЮА, 2012. № 3 (84). С. 131.

другие, способствующие раскрытию признаков состава преступления: понятие субъекта, вины и др.). Таким образом, состав преступления, будучи *правовым* основанием для квалификации преступления, не является ее единственным источником[32].

Известно, что диспозиции некоторых уголовно-правовых норм, в которых формулируются признаки соответствующих составов преступлений, сконструированы в качестве *бланкетных*. При квалификации деяний подобного рода правоприменитель вынужден обращаться к нормам *других* отраслей права. Отношение к этим предписаниям, как правовой базе для квалификации преступлений, сложилось в теории уголовного права неоднозначное. Составляя правовую базу, нормы других отраслей права не могут, по нашему мнению, быть самостоятельной основой для квалификации преступления, ибо при квалификации ссылка на них не делается. Они необходимы для правильного толкования содержания соответствующих составов преступлений. К примеру, для правильного понимания регламентированных бланкетными нормами правил эксплуатации и правил доступа к средствам компьютерной техники (ч. 1 ст. 274, ч. 3 ст. 274^1 УК РФ). Гражданско-правовые и конструкции иных отраслей права, используемые законодателем при описании определенных видов преступлений, имеют важное значение для характеристики соответствующих составов преступлений. Они являются составной частью правовой базы, на которую опирается правоприменитель при квалификации преступления, но не могут, на наш взгляд, рассматриваться как ее юридическая основа (в узком понимании этого термина). Квалификация преступления, которая представляет собой особый вид уголовно-правовой оценки, реализует себя в ссылке на статью (часть, пункт) УК РФ.

Таким образом, действительной уголовно-правовой основой для квалификации преступления является состав преступления как законодательная

---

[32] Р. А. Сабитов полагает, что юридическая основа уголовно-правовой квалификации – это источники уголовного права, на которых основывается квалификация деяний и событий, а также иные нормативные явления, которые используются при их уголовно-правовой оценке. См.: Сабитов Р. А. Указ. соч. С. 120.

модель преступления определенного вида, а в указанных законом случаях также иные правовые предписания УК РФ, содержащиеся в его Общей части.

§ 2. Состав преступления, его виды и алгоритм квалификации преступного деяния

Состав преступления – это «предусмотренная уголовным законом система объективных и субъективных признаков, характеризующих общественно опасное деяние как определенный вид преступления»[33], хотя его определение не всегда излагается подобным образом. В литературе существуют и иные подходы к характеристике этой уголовно-правовой категории. О составе преступления в теории уголовного права нередко говорят как о законодательной модели преступления, юридическом понятии, как о научной (теоретической) конструкции, доктринальном образе определенного деяния. Действительно, понятие состава преступления имеет процессуальные корни (corpus delicti) и стало использоваться в уголовном праве как некая конструкция, позволяющая дать характеристику определенному виду преступления и отграничить его от другого.

Трудно согласиться с тем, что в реальности существуют два состава: как законодательная модель и как состав, содержащийся в самом деянии как фактическое основание квалификация преступления. Выдающийся криминалист Н. Ф. Кузнецова писала, что имеется «фактический состав» содеянного и «юридический состав» преступления[34]. Эта позиция поддерживается в теории[35]. На наш взгляд, содеянное заключает в себе совокупность фактических данных, которые преобразуются правоприменителем в юридически значимые (уголовно-правовые).

Понятие «состав преступления» необходимо отличать от понятия «преступление». Понятие «преступление» излагается в ст. 14 УК РФ: это виновно

---

[33] Уголовное право России. Общая часть: Учебник / Под ред. Ф. Р. Сундурова, И. А. Тарханова. 2-е изд., перераб. и доп. М.: Статут, 2016. С. 197. (автор главы – Тарханов И. А.).
[34] См.: Кузнецова Н. Ф. Указ. соч. С. 18.
[35] См.: Сабитов Р. А. Указ. соч. С. 176.

совершенное общественно опасное деяние, запрещенное Уголовным кодексом под угрозой наказания. Таким образом, рассматриваемое понятие включает в себя как социальные, так и юридические признаки, свойственные любому виду преступления. Это позволяет отгранивать преступление от иных противоправных деяний (правонарушений) и общественно вредных (антисоциальных) поступков. В ч. 2 ст. 14 УК РФ дается понятие малозначительного деяния (действия или бездействия), которое преступлением не является, хотя формально и содержащее признаки какого-либо деяния, предусмотренного УК РФ.

Как отмечалось ранее, состав преступления как законодательная модель (конструкция) позволяет отграничивать один *вид* преступления от другого. Так, в главе 28 УК РФ содержится описание (указание на признаки) четырех видов преступлений против безопасности компьютерной информации. Система признаков, свойственная каждому из них, образует законодательную модель определенного вида преступления. С их помощью (на их основе) они отграничиваются друг от друга. К примеру, лицом может быть создана вредоносная компьютерная программа (далее – ВКП), а затем распространена. С позиции обывателя совершается несколько преступлений. Однако, по правилам квалификации с учетом признаков непосредственного объекта и в особенности объективной стороны состава преступления, такое деяние рассматривается в качестве единичного, хотя и сложного по характеристике преступления.

Указание на состав преступления как систему объективных и субъективных признаков позволяет рассматривать их как взаимосвязанные между собой. Нередко уголовно-правовая характеристика отдельно взятого признака (к примеру, субъективного) состава преступления позволяет раскрыть содержание другого (к примеру, субъективного) признака состава преступления. Такой подход позволяет выявить структуру состава конкретного вида преступления в полном объеме.

Структуру состава преступления образуют ряд уголовно-правовых признаков [36], которые характеризуют внешнюю и внутреннюю сторону

[36] Некоторые ученые полагают, что признаки состава преступления предусматриваются в других (не уголовных) законах. См., напр.: Гаухман Л. Д. Указ. соч. С. 48. Следует согласиться с Р. А. Сабитовым, что признаки состава

конкретного деяния. В теории их принято группировать по таким *элементам* состава преступления, как объект преступления и его объективная сторона, субъект и субъективная сторона. Законодатель использует различные способы формирования состава преступления как информационной модели для квалификации преступления. С учетом этого *составы преступлений классифицируются* по различным основаниям.

Одним из оснований такой классификации является *оценка* законодателем *степени* общественной опасности определенного деяния. Поэтому их подразделяют на основные, привилегированные, квалифицированные и особо квалифицированные составы преступлений. Первый вид состава преступления заключает в себе сущностные (общие) признаки, отражающие специфику данного вида преступления по отношению к другим. Законодательное описание признаков основного состава преступления обычно излагается в начальных (первых) частях соответствующих статей Особенной части УК РФ. Однако законодатель не всегда следует этому подходу. Квалифицированные составы преступлений (с отягчающими обстоятельствами) содержат помимо сущностных признаков обстоятельства, существенно повышающие общественную опасность деяния (обычно это вторые части составов преступлений). Особо квалифицированные составы преступления – обстоятельства, придающие совершенному деянию особую опасность (обычно части третьи и последующие). Привилегированные составы преступлений (со смягчающими обстоятельствами) содержат в себе признаки, уменьшающие степень общественной опасности преступления. Так, состав преступления, изложенный в ч. 1 ст. 272 УК РФ, является основным составом неправомерного доступа к компьютерной информации. В то же время в ст. 274^{1} УК РФ характеристика основных составов излагается законодателем в частях 1, 2 и 3 данной статьи. Состав преступления, изложенный в ч. 2 ст. 272 УК РФ, является квалифицированным. Составы преступлений, сформулированные в ч.

преступления указаны в УК РФ, а нормы других отраслей права используются для толкования и раскрытия содержания тех или иных признаков состава преступления. См.: Сабитов Р. А. Указ. соч. С. 178.

3 и ч. 4 ст. 272 УК РФ, – особо квалифицированными. Привилегированных составов рассматриваемых нами преступлений законодательство не содержит.

По особенностям конструирования *объективной стороны* составы преступлений подразделяют обычно на формальные и материальные. Некоторые авторы выделяют среди первых усеченные составы преступления[37]. Обычно их рассматривают как самостоятельные виды.

Для материального состава преступления характерно, что в качестве обязательного признака их объективной стороны предусматриваются общественно опасные последствия деяния, которые предполагают установление причинной связи между деянием и данным последствием. Объективная сторона преступления в формальных составах описывается путем указания только на само действие (или бездействие) [38] , т.е. содержит описание самого уголовно-наказуемого поступка.

Четыре основных состава преступления против безопасности компьютерной информации, признаки которых излагаются в ч. 1 ст. 272, ч.1 ст. 274 УК РФ, части 2 и 3 ст. 274^1 УК РФ, являются по своей конструкции материальными, а два основных состава, изложенных в ч. 1 ст. 273 УК РФ, ч. 1 ст. 274^1 УК РФ, – формальными.

В литературе принято считать, что установление вида состава преступления с учетом специфики конструирования законодателем их объективной стороны (формальный, материальный или усеченный состав преступления) способствует установлению момента юридического окончания преступления, времени совершения преступления, установление возможности добровольного отказа от доведения преступления до конца, определения формы вины, множественности преступлений, исчисления сроков давности и т.д.[39] С этим следует согласиться.

Составы преступлений по особенностям их внутренней *структуры* подразделяют обычно на *простые* и *сложные*. В отличие от простых составов, их

---

[37] См.: Уголовное право России. Общая часть: Учебник / Под ред. Ф. Р. Сундурова, И. А. Тарханова. 2-е изд., перераб. и доп. М.: Статут, 2016. С. 207.
[38] См.: Гаухман Л. Д. Указ. соч. С. 55.
[39] Соктоев З. Б. Причинность и объективная сторона преступления: Монография. М.: НОРМА, ИНФРА-М, 2015. С. 14.

сложные разновидности заключают в себе либо несколько объектов, несколько разнородных деяний, разнородных или альтернативных последствий, характеризуются двумя формами вины, либо сочетанием названных признаков. Все составы преступлений против безопасности компьютерной информации конструктивно являются сложными составами преступлений, но отличающимися по различным составляющим.

До настоящего времени нет однозначного понимания по вопросу происхождении термина «алгоритм». По одному из источников, он происходит от латинской транслитерации имени аль-Хорезми среднеазиатского математика IX в. и означает систему правил (предписаний) для эффективного решения задач[40]. По другой версии, происходит от арабского имени собственного «Algorithmi», и под ним понимается «понятное и точное предписание исполнителю совершить последовательность действий, направленных на достижение указанной цели или на решение поставленной задачи»[41]. Как указывает Р. А. Сабитов, алгоритм – это «система операций, применяемых по строго определенных правилам, которая после последовательного их выполнения приводит к решению поставленной задачи»[42].

Таким образом, *алгоритм квалификации преступления* – это последовательность действий правоприменителя при квалификации преступлений. Частично проблема алгоритмизации была рассмотрена при изложении содержания квалификации как деятельности. В данном фрагменте работы тема алгоритмизации предполагается для исследования последовательности при установлении отдельных элементов состава преступления в процессе его квалификации. Поэтому алгоритм квалификации преступления следует различать от вышерассмотренных этапов квалификации преступлений как совокупности логико-юридических операций. В теории квалификации преступления представляется возможным выделить два основных подхода к алгоритмизации квалификации преступления с

---

[40] Философский энциклопедический словарь / Гл. редакция: Л. Ф. Ильичев, П. Н. Федосеев, С. М. Ковалев, В. Г. Панов. М.: Советская энциклопедия, 1983. URL: http://dic.academic.ru/dic.nsf/enc_philosophy/4131/АЛГОРИТМ.

[41] Словарь иностранных слов. / Н. Г. Комлев М.: Эксмо, 2006. URL: http://dic.academic.ru/dic.nsf/dic_fwords/3334

[42] Сабитов Р. А. Указ. соч. С. 67.

точки зрения последовательности выявления элементов состава преступления. Одни авторы предлагают начинать квалификацию преступления с установления объекта уголовно-правовой охраны и преступления[43]. Н. К. Семернева полагает, что вначале необходимо установить объект преступления по той причине, что его отсутствие исключает само преступление[44]. Думается, что допустимо иное обоснование. Правильное установление названных объектов облегчает поиск нужной уголовно-правовой нормы и состава в уголовно-правовом массиве. Система Особенной части УК РФ, ее структура построена с учетом объекта уголовно-правовой охраны: на этой основе выделяются не только ее разделы, но и подразделяются главы. Существующее построение Особенной части УК РФ способствует эффективному выстраиванию квалификационных версий, формированию уголовно-правовой базы.

Ряд авторов исходит из того, что квалификацию преступления следует начинать с установления объективной стороны состава преступления как «видимой», очевидной, поддающейся непосредственному восприятию. Однако и объект преступления может быть познан правоприменителем непосредственно, к примеру, через предмет посягательства, т.е. методологически тем же путем через познание объективной деятельности, социальных фактов. Л. Д. Гаухман предлагает начинать процесс квалификации преступления с объективной стороны преступления по той причине, что она наиболее полно отражена законодателем, затем, по его мнению, следует устанавливать признаки субъекта, субъективной стороны и объекта преступления[45]. По мнению Е. В. Благова, алгоритм квалификации преступления, выраженный в схеме «объективная сторона -> объект -> субъект -> субъективная сторона», считается приемлемым потому, что отсутствие любого из предыдущих признаков завершает квалификацию[46].

В доктрине существовали подходы, согласно которым в некоторых случаях вовсе не обязательно следовать заранее четко построенному алгоритму

---

[43] Кудрявцев В. Н. Указ. соч. С. 130. Гаухман Л. Д. Указ. соч. С. 313.
[44] Семернева Н. К. Указ соч. С. 36.
[45] Гаухман Л. Д. Указ. соч. С. 315-316.
[46] Благов Е. В. Применение уголовного права (теория и практика). СПб.: Юридический центр Пресс, 2004. С. 115.

квалификации, что подвергается критике и представляется не весьма убедительным, а на практике приводит к ошибкам в квалификации[47].

Таким образом, следует согласиться с тем, что проблема алгоритмизации квалификации преступлений остается актуальной[48]. Тем более, что существуют еще и эвристические модели построения квалификации [49] . Квалификацию преступления, по нашему убеждению, следует начинать с установления объектов уголовно-правовой охраны и преступления. Далее переходить к установлению объективной стороны состава преступления и совершенного деяния. Анализ содержания субъективной стороны состава и деяния методологически связан с характеристикой объективных признаков состава и социальных фактов, составляющих объективную сторону содеянного. Признаки субъекта преступления устанавливаются с учетом специфики конкретного деяния. Изложенные соображения в определенной степени обусловили содержание и структуру третьей главы настоящей работы.

§ 3. Правила квалификации преступления и критерии деления их на виды

В. Н. Кудрявцевым впервые в теорию квалификации преступления введено понятие «правильной квалификации преступления». В сущности эта новация наметила основные векторы концептуального и фундаментального по характеру исследования *правил* квалификации преступления. К сожалению, имеющиеся в современной уголовно-правовой доктрине подходы к определению самого понятия, их видам, содержанию нельзя признать удовлетворительными.

Согласно точке зрения А. В. Корнеевой, под правилами квалификации понимается «предписание, устанавливающее порядок действий правоприменителя при известных фактических обстоятельствах для выбора при квалификации

---

[47] Кудрявцев В. Н. Указ. соч. С. 207.
[48] См.: Сабитов Р. А. Указ. соч. С. 63.
[49] См.: Кудрявцев В. Н. Общая теория квалификации преступлений. М., 1972. С. 196.

преступления конкретного пункта, части, статьи УК РФ»[50]. Н. Т. Идрисов, посвятивший данной теме свою кандидатскую диссертацию, обратил внимание юридической общественности на отсутствие единого официального источника, регламентирующего осуществление квалификации преступления по определенным правилам. В связи с этим автор предлагает ввести в УК РФ новую главу, посвященную правилам квалификации преступления, а также принять Свод правил квалификации[51].

В. К. Дуюнов, обобщив правила квалификации преступлений, понимает под ними «выработанные наукой уголовного права и (или) правоприменительной практикой и отчасти воплощенные в уголовном законодательстве *положения* (требования), определяющие пути и способы правильной квалификации (законной, обоснованной и наиболее точной) оценки совершенного лицом общественно опасного деяния как конкретного преступления *или как деяния, не содержащего признаков преступления* (курсив наш – Р. Г.)»[52]. Соглашаясь с подходом к оценке правил как некоторых положений (носящих характер требований), следует возразить против включения в понятие квалификации отграничение преступного от непреступного. И. А. Тарханов прав, по нашему мнению, выводя оценку деяния в качестве не содержащего признаков преступления за рамки понятия квалификации преступления. Это уголовно-правовая квалификация, но другого вида. Отграничение преступного от непреступного не есть квалификация преступления. Очевидно и по этой причине квалификация преступления не может быть негативной, как считают некоторые ученые. Если имеет место преступление, то при его квалификации необходимо правильно установить его вид, и такая оценка является позитивной. Кроме того, правила отграничения преступного от непреступного как разновидности уголовно-правовой квалификации могут и, очевидно, должны отличаться от правил квалификации преступления, понимаемой как установление его вида.

---

[50] Корнеева А. В. Указ. соч. С. 25.
[51] Идрисов Н. Т. Правила квалификации преступлений: понятие, виды, проблема правового регулирования : дис. … канд. юрид. наук. Самара, 2009. С. 11, 63.
[52] Дуюнов В. К., Хлебушкин А. Г. Указ. соч. С. 11.

Н. Т. Идрисов справедливо, на наш взгляд, подчеркивает, что правила квалификации преступлений не следует отождествлять с основополагающими идеями, коими являются принципы, и с элементарной методикой применения закона, которую также следует отличать от правил квалификации[53].

Значение правил квалификации преступления, как справедливо отмечает Л. Д. Гаухман, заключается в том, что их соблюдение обеспечивает точную (правильную, в смысле – соответствующую правилам) квалификацию преступления, и посредством этого реализацию уголовной политики государства, выраженной и закрепленной в уголовном законодательстве [54] . Значимость правильной квалификации преступления проявляется и в ее социально-правовых последствиях, которая она за собой влечет. С социально-нравственной стороны она выражается в отношении виновного к определенному классу, страте людей. В литературе справедливо выделяются также уголовно-правовые последствия (возможность применения санкций, установление сроков давности, решение вопросов об условно-досрочном освобождении, замены наказания) и уголовно-процессуальные (избрание меры процессуального пресечения, форму проведения расследования, возбуждение уголовного дела, подследственность дела и его подсудность) значения квалификации преступлений[55]. К примеру, уголовные дела о неправомерных воздействиях на критическую информационную инфраструктуру Российской Федерации (далее – КИИ РФ), в отличие от иных дел о преступлениях против безопасности компьютерной информации с 1 янв. 2018 г. будут подследственны органам федеральной службы безопасности.

А. В. Корнеева справедливо исходит из того, что при определении понятия «правило квалификации преступлений» необходимо определиться в этимологической составляющей изначального термина. «Правило» – это положение, отражающее некую закономерность, постановление, предписание, устанавливающее порядок чего-нибудь[56]. Квалификация преступления является,

---

[53] Идрисов Н. Т. Указ. соч. С. 65.
[54] Гаухман Л. Д. Указ. соч. С. 268.
[55] См.: Сабитов Р. А. Указ. соч. С. 11.
[56] Корнеева А. В. Указ. соч. С. 24.

правильной, если она осуществляется в соответствии с существующими (действующими), общеобязательными (утвержденными) правилами. Следует согласиться с мнением, что правила официальной квалификации *обращены* к правоприменителю (это правило поведения субъекта квалификации)[57]. Правило – это предписание, которое подлежит исполнению. В противном случае квалификация преступления окажется неправильной (к примеру, неполной либо избыточной). Содержание правила должно заключать в себе *образ действий* правоприменителя при наличии определенной ситуации. И наконец, относительно какой сферы деятельности существуют правила квалификации преступления? Ответ на этот вопрос не настолько очевиден, как представляется поначалу. По мнению Р. А. Сабитова, это правила «по установлению и юридическому закреплению соответствия признаков фактического состава признакам уголовно-правового состава»[58]. Мнение А. В. Корнеевой несколько отличается от данного вывода. Она полагает, что это «*предписание*, *устанавливающее порядок* (выделено нами – Р. Г.) действий правоприменителя при известных фактических обстоятельствах для выбора при квалификации преступления конкретного пункта, части, статьи УК РФ»[59]. Иными словами, эти правила имеют вполне конкретное назначение – правильно определиться со ссылкой на уголовный закон, т.е. речь идет о квалификации преступления в узком ее значении (понимании). В этом утверждении скрывается своя логика и некоторые ее обоснования, с которыми, в принципе, следует согласиться, оставляя возможность для оговорок. В русском языке термин «образ» имеет много значений. Одно из них «способ, вид, облик», хотя включает в себя и «порядок», но последний определяется так же, как «последовательный ход чего-то»[60]. В связи с этим алгоритм квалификации преступления не является обязательным положением в силу отсутствия указания на это в нормативном акте и дискуссионности проблемы в науке.

---

[57] См.: Сабитов Р. А. Указ. соч. С. 231.
[58] Там же.
[59] Корнеева А. В. Указ. соч. С. 25.
[60] Толковый словарь русского языка под ред. С. И. Ожегова и Н. Ю. Шведовой. М., 1997. URL: http://dic.academic.ru/dic.nsf/ogegova/278181 (дата обращения: 17.07.17).

Поэтому под правилами официальной квалификации преступлений представляется возможным понимать нормативные, а также 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.

Правила квалификации можно классифицировать по различным критериям (основаниям). По *количественному* признаку (из большего или меньшего круга квалифицируемых деяний) Л. Д. Гаухман классифицирует их на общие (они используются при квалификации всех без исключения деяний), частные (специальные), единичные (правила разграничения конкретных видов преступлений). *Качественный* критерий, согласно идее автора, применим только в научных и учебных целях. Его сутью является отнесение правил к тому или иному разделу уголовного права.

В качестве *общих* автором выделяются правила, основывающиеся на принципах, отраженных в Уголовном кодексе Российской Федерации, Конституции Российской Федерации и на иных положениях, регламентированных в Уголовном кодексе Российской Федерации. К их числу Л. Д. Гаухман относит ряд таких правил[61]. Р. А. Сабитов отмечает, что такой перечень общих правил подвергается критике как некорректный, ибо эти положения в действительности не являются правилами, а касаются иных институтов уголовного права[62]. С этим следует согласиться.

Частные (специальные) правила, которые применяются к определенным типичным случаям, Л. Д. Гаухманом сгруппированы также по качественным признакам: в отношении отдельного состава преступления (связанные с

---

[61] 1) Содеянное должно быть предусмотрено уголовным законом в качестве преступления; 2) оно должно содержать конкретный состав преступления; 3) официальная квалификация деяния базироваться на точно установленных и доказанных фактических данных; 4) преступление квалифицируется по уголовному закону, действовавшему во время совершения преступления; 5) временем совершения преступления признается время совершения деяния; 6) по УК РФ квалифицируется деяние, совершенное на территории Российской Федерации; 7) в отдельных случаях (ст. 12 УК) могут по УК РФ квалифицироваться деяния, совершенные вне пределов РФ. См. подробнее: Гаухман Л. Д. Указ. соч. С. 275-283.

[62] См.: Сабитов Р. А. Указ. соч. С. 233.

особенностями субъективных признаков преступлений, квалификацией неоконченной преступной деятельности, соучастия в преступлении, мнимой обороны), при множественности преступлений (правила квалификации при конкуренции общей и специальной норм, части и целого, совокупности преступлений), а также при изменении квалификации преступлений.

Единичные – безграничные, определяемые в процессе анализа конкретных составов преступлений и их разграничении (например, при отграничении уничтожения или повреждения чужого имущества от некоторых видов преступлений против безопасности компьютерной информации)[63].

А. В. Корнеева исходит из того, что выделение неких единичных правил квалификации «вообще дезавуирует понятие правил квалификации преступлений», а множественность преступлений и конкуренцию уголовно-правовых норм следует рассматривать в качестве самостоятельных уголовно-правовых институтов, которые регламентируются различными правилами [64] . Поэтому подвергает предложенную классификацию критике. Р. А. Сабитов присоединяется к этой позиции, поскольку считает, что правила, предлагаемые Л. Д. Гаухманом, сгруппированы без единого критерия. По его собственной классификации, в качестве *оснований* группировки рассматриваемых правил следует заложить элемент состава преступления, и разделить их на правила квалификации соответственно по объекту преступления, его объективной и субъективной стороне и субъекту преступления. При выборе в качестве основания *количество* квалифицируемых деяний, выделить правила квалификации единичного преступления и множества преступления. По степени *завершенности* преступной деятельности выделить правила квалификации неоконченного преступления и оконченного. С учетом *количества лиц*, участвующих в совершении преступления, различать правила квалификации уголовно-правовых деяний, совершенных единолично исполнителем и совершенных в соучастии[65].

---

[63] Гаухман Л. Д. Указ. соч. С. 271-273.
[64] Корнеева А. В. Указ. соч. С. 25.
[65] Сабитов Р. А. Указ. соч. С. 233-234.

Нам представляется рациональной классификация правил квалификации преступлений, предлагаемая 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 им относятся правила квалификации неоконченных преступлений, деяний, совершенных в соучастии, при множественности преступлений, конкуренции уголовно-правовых норм и др.[66]

[66] Рарог А. И. Указ. соч. С. 51.

Глава 2. Социально-правовая обусловленность уголовной ответственности за посягательства на безопасность компьютерной информации

§ 1. Понятие компьютерной информации и преступления против ее безопасности

С середины XX в. «информация», как категория, начинает проникать в науки, не связанные с математикой. В настоящее время понятие «информация» является общенаучным. Понятие «информация» широко используется во всех общественных сферах деятельности человека: в науке, технике, культуре, социологии, а также на обыденном уровне. Общепринято считать, что термин «информация» образован от латинского слова «informatio», в переводе означающее разъяснение, изложение, истолкование, осведомление, представление, понятие, осведомление и просвещение[67].

Информация является предметом изучения как социальных, так и естественных наук. Одной из основных естественных наук, связанной с рассматриваемой проблемой, является информатика[68]. Для понимания сущности развивающихся современных информационных процессов немаловажное значение имеют положения и других естественных наук, таких, как кибернетика, математика, физика, химия, электроника, радиотехника и др. Однако справедливо указывается, что науки естественного цикла заимствовали понятие «информация» из гуманитарных наук[69].

В доктрине ведутся дискуссии по вопросу что понимать под термином «информация»[70]. Теорией философского познания (гносеологией) предлагаются разнообразные подходы к ее определению. В ее рамках существуют две

---

[67] См., напр.: Воройский Ф. С. Информатика. Новый систематизированный толковый словарь-справочник. М.: Физматлин, 2003. С. 14; Информационное право: Учебник / Л. Л. Попов, Ю. И. Мигачев, С. В. Тихомиров. М.: Норма: ИНФРА-М, 2010. С. 14; Подосинов А. А. Русско-латинский словарь [Электронный ресурс] / А.В. Подосинов, А. М. Белов. 5-е изд., стер. М.: Флинта, 2011. С. 91; Маскаева А. М. Основы теории информации: Учебное пособие / А.М. Маскаева. М.: Форум: НИЦ ИНФРА-М, 2014. С. 8.

[68] Информатика – наука о методах и процессах сбора, хранения, обработки, передачи, анализа и оценки информации с применением компьютерных технологий, обеспечивающих возможность ее использования для принятия решений. Журавлев Ю. И., Гуревич И. Б. ИНФОРМАТИКА // Большая российская энциклопедия. Электронная версия (2016). URL: http://bigenc.ru/mathematics/text/2015747 (дата обращения: 17.07.2017).

[69] Урсул А. Д. Проблема информации в современной науке. Философские очерки. М.: Наука, 1975. С. 15.

[70] См., напр.: Сотов А. И. Компьютерная информация под защитой. Правовое и криминалистическое обеспечение безопасности компьютерной информации. М.: Русайнс, 2015. С. 4.

противоположные концепции информации: атрибутивная и функциональная[71]. Названные концепции понимают информацию как отраженное разнообразие. Их различие заключается в вопросе относимости информации к классу объектов и явлений. Атрибутивная концепция определяет информацию как структурное, организованное, упорядоченное свойство движущейся материи. Иными словами, информация рассматривается как качество всех материальных объектов. В функциональной концепции информации придается свойство конкретного класса в материальных системах. При этом к материальным системам относят 1) живые организмы и их сообщества, 2) человека и социум, 3) автоматические (компьютерные) системы управления[72]. Атрибутивная и функциональная концепции одновременно признают наличие двух видов информации: в живой и неживой природе. Если обработка информации в неживой природе характеризуется пассивностью и отсутствием разнообразия направленности информации, то в живой природе ей характерны многоуровневость, избирательность и адекватность[73].

В теории информации и информатике «информация» рассматривается как «отражение реального, материального, предметного мира, выражаемое в сигналах и знаках»[74], «последовательность сигналов, передаваемых от передатчика к приемнику, накопляемых в запоминающем устройстве, обрабатываемых и выдаваемых в виде готовых результатов»[75], «известия, сообщения, сведения, адекватно отражающие объективную действительность и позволяющие узнать что-то новое, ранее неизвестное, или подтвердить известное в целях принятия правильного решения»[76].

Информация как фундаментальное понятие включает в себя синтаксические, семантические и прагматические свойства. Перечисленные аспекты информации

---

[71] См.: Урсул А. Д. Указ соч. С. 54-62; Гришкин И. И. Понятие информации. Логико-методологический аспект. М.: Наука, 1973. С. 12; Абдеев Р. Ф. Философия информационной цивилизации. М.: ВЛАДОС, 1994. С. 160-162.

[72] См.: Юрченко И. А. Информация конфиденциального характера как предмет уголовно-правовой охраны : дис. … канд. юрид. наук. М., 2000. С. 20.

[73] Там же.

[74] Маскаева А. М. Указ. соч. С. 7.

[75] Кольман Э. Я. Указ. соч. С. 5.

[76] Информационное право: Учебник / Л. Л. Попов, Ю. И. Мигачев, С. В. Тихомиров. М.: Норма: ИНФРА-М, 2010. С. 14, 18.

открывались наукой в соответствующем хронологическом порядке. А. Б. Венгеров, проведя анализ синтаксического, семантического и прагматического подходов к определению информации, констатировал наличие соответствующих этапов, стадий, «фильтров» при передаче информации, которая «всегда сначала принимается, затем понимается, потом оценивается, и, наконец, используется»[77]. Указанные аспекты впервые были собраны кибернетикой (как наукой) под единым знаменателем, в котором был выдвинут тезис о важности их рассмотрения в совокупности. Синтаксические, семантические и прагматические характеристики информации отражают соответственно основные свойства информации как содержание, форму и ценность информации. Изучение компьютерной информации в рамках уголовного права, как нам представляется, также необходимо в единстве названных характеристик, признаков и свойств, которые отображают общепринятый подход к проблеме определения сущности информации.

На наш взгляд, наиболее значимой классификацией среди выделяемых в доктрине и законодательстве видов информации для уголовного права представляют классификации: 1) по форме ее представления, 2) по своей значимости (прежде всего социальной и экономической), 3) по основанию порядка распространения и (или) ее предоставления; 4) по способу обработки[78]. Свойства информации, объединяемые указанными классификациями, являются криминообразующими признаками, и их уяснение имеет существенное значение для разрешения проблем юридической техники и квалификации преступлений.

1. Классификация по форме представления информации. Для возможности восприятия субъектом любой информации необходимо ее закрепление в определенной форме. В качестве таких форм выступают текстовые, числовые, графические, аудио либо комбинированные формы представления информации.

---

[77] Венгеров А. Б. Категория «информация» в понятийном аппарате юридической науки // Советское государство и право. М.: Наука, 1977. № 10. С. 70-78.

[78] См., напр.: 7. Об информации, информационных технологиях и о защите информации : федер. закон Рос. Федерации от 27 июля 2006 г. № 149-ФЗ : принят Гос. Думой Федер. Собр. Рос. Федерации 08 июля 2006 г. : одобр. Советом Федерации Федер. Собр. Рос. Федерации 14 июля 2006 г. // Собр. законодательства Рос. Федерации. 2006. № 31 (1 ч.), ст. 3448; Маскаева А. М. Указ. соч. С. 9; Лопатин В. Н. Информационная безопасность России : дис. … д-ра юрид. наук. СПб, 2000. С. 48.

Именно свойство «формы представления» информации законодатель заложил в качестве основного признака определения «компьютерной информации», содержащейся в УК РФ. Согласно примечанию 1 к ст. 272 УК РФ, «под компьютерной информацией понимаются сведения (сообщения, данные), представленные в *форме* (курсив наш – авт.) электрических сигналов, независимо от средств их хранения, обработки и передачи».

Следует сказать, что электрические сигналы являются одной из форм, при которой они могут быть обработаны электронными устройствами (в т.ч. компьютерной техникой), а сама информация может быть представлена и в других (неэлектронных) формах, но в то же время считываться компьютерными устройствами ввода и вывода и преобразовываться в электронную информацию (т.е. обрабатываться).

2. *Классификация по значимости информации*. Информация только при определенных обстоятельствах приобретает признак значимости. Такой признак делает информацию общественно значимой и, следовательно, материально обосновывающей ее уголовно-правовую охрану. Общественная значимость информации приобретает немаловажное значение для определения материальной ценности информации, а также является одним из признаков относимости информации к конфиденциальной.

Из признака общественной значимости вытекает следующий необходимый критерий для криминализации общественно опасного посягательства на информацию – ее экономическая ценность, которая не перестает возрастать в информационном обществе[79].

3. Классификация по категории доступа и порядку предоставления и распространения информации. В Федеральном законе № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – ФЗ № 149-ФЗ) приняты за основу классификации информации:

- категория предоставляемого доступа;

[79] См.: Геллер А. В. Уголовно-правовые и криминологические аспекты обеспечения защиты электронной информации и Интернета: автореф. дис. … канд. юрид. наук. М., 2006. С. 7.

- порядок предоставления или распространения;

- содержание информации или вид ее обладателя[80].

Данная классификация соответствует в том числе и международно-правовым документам. Так, в частях 2 и 3 ст. 19 Международного пакта о гражданских и политических правах закрепляются принципы свободы поиска, получения и распространения всякого рода информации, а также ограничение в обороте информации, необходимой для уважения прав и репутации других лиц и охраны государственной безопасности, общественного порядка или нравственности населения[81].

4. Классификация по способу обработки информации. Информация всегда передается материально: свет, радиоволны, звук, электричество – во всех перечисленных способах передачи сигналов задействовано передвижение материи [82] . Способ передачи лежал в основе определения компьютерной информации в ч. 1 ст. 272 УК РФ в первоначальной редакции УК 1996 г., из которой путем ее толкования следовало, что под ней понималась информация на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети.

Сегодня «информация» является признаком конструктивных элементов не только составов преступлений, регламентирующих ответственность за рассматриваемые нами в данной работе виды преступлений, но и многих других. Это обусловливает необходимость проведения анализа понятия «информация» и в юридической литературе.

Так, А. М. Маскаева отмечает, что «в рамках науки информация является первичным и неопределяемым понятием … Конкретное толкование элементов, связанных с понятием «информация», зависит от метода конкретной науки, цели

---

[80] См.: Об информации, информационных технологиях и о защите информации : федер. закон Рос. Федерации от 27 июля 2006 г. № 149-ФЗ : принят Гос. Думой Федер. Собр. Рос. Федерации 08 июля 2006 г. : одобр. Советом Федерации Федер. Собр. Рос. Федерации 14 июля 2006 г. // Собр. законодательства Рос. Федерации. 2006. № 31 (1 ч.), ст. 3448.

[81] См.: Международный пакт о гражданских и политических правах от 16 дек. 1966 г. : принят Резолюцией 2200 (XXI) на 1496-ом пленарном заседании Генеральной Ассамблеи ООН 16 дек. 1966 г. // Ведомости Верховного Совета СССР. 1976. № 17, ст. 291. URL: http://consultant.ru/ (дата обращения: 17.07.17).

[82] См.: Кольман Э. Я. О философских и социальных идеях Норберта Винера // Кибернетика и общество. М.: Издательство иностранной литературы, 1958. С. 16.

исследования или просто от наших представлений»[83]. Такой вывод в дальнейшем мы можем наблюдать и в других работах, в том числе посвященных уголовно-правовому анализу исследуемого понятия. Особенным свойством информации является способность ее, преломляясь в разнородных общественных отношениях, обретать новые признаки[84].

А. И. Сотов, придерживаясь взглядов основоположника теории информации К. Шеннона, определяет информацию как «любой сигнал (независимо от его физической природы), исходящий от объектов материального мира, на основании которого субъекты поведения могут совершать определенные самостоятельные действия»[85]. И. А. Юрченко, рассмотрев философские и правовые аспекты понятия «информация», пришла к выводу, что объектом правового регулирования является идеальная информация социального вида, под которой понимается «обозначение содержания, полученного из внешнего мира в процессе приспособления к нему наших органов чувств»[86]. Такое определение в общих чертах коррелируется и с нашим пониманием информации.

В нормативно-правовых актах и в литературе наряду с понятием «информация» используются и другие понятия. Так, законодатель в ст. 2 ФЗ № 149-ФЗ «информацию» определяет, как «сведения (сообщения, данные) независимо от формы их представления». Следовательно, законодателем они употребляются в качестве тождественных понятий. Ранее в законодательстве отождествлялись только понятия «информация» и «данные»[87]. В УК РФ наряду с понятием «информация» также используются понятия «сведения», «сообщения», «данные». Проведя анализ литературы, мы сталкиваемся с мнениями как об их тождественности, так и об их различии[88].

---

[83] Маскаева А.М. Указ. соч. С. 8.
[84] См.: Там же; Геллер А. В. Указ. соч. С. 10-11.
[85] Сотов А. И. Указ. соч. С. 5.
[86] Юрченко И. А. Указ. соч. С. 28.
[87] См.: ст. 2 Федерального закона от 20.02.1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» // Собр. законодательства Рос. Федерации. 1995. № 8, ст. 609. (утр. силу).
[88] См., напр.: Юрченко И. А. Там же; Воройский Ф. С. Указ. соч. С. 13; Яшков С. А. Информация как предмет преступления: дис. ... канд. юрид. наук. Екатеринбург, 2005. С. 8.

Нами проведено исследование степени проникновения того или иного понятия в нормы УК РФ (см. *Приложение 3 и 4*). Так, на понятие «информация» указывается в нормах Общей части УК РФ[89], при конструировании составов преступлений в Особенной части УК РФ[90], а также в определениях «средства массовой информации»[91] и «информационно-телекоммуникационной сети»[92].

Понятие «сведения» используется законодателем в одной норме Общей части УК РФ[93], при конструировании составов преступлений Особенной части УК РФ [94] . Под «сведениями» понимаются «факты, данные, характеризующие кого-либо, что-либо»[95]. По своей сущности информация и отображаемый ею объект взаимодействуют в виде некоего отношения. Составляющими такого отношения являются сам факт, информация о нем и принимающий субъект. Сведения являются значимыми для принимающего его субъекта. Без субъекта восприятия сведения остаются лишь информацией. В неживой природе информация элементарно отражает информацию об одном объекте относительного другого без участия субъекта ее восприятия и без переработки. Поэтому, как справедливо утверждает А. М. Маскаева, понятие «информация» шире понятия «сведения»[96].

В ФЗ № 149-ФЗ понятия «сведения» и «информация» обозначены в качестве равнозначных. Однако, как справедливо полагает И. А. Юрченко, такое положение является верным только по отношению к социальной идеальной информации[97]. А. В. Минбалеев утверждает, что понятия «данные» и «сообщения» являются разновидностью сведений[98]. Таким образом, в сущности сведения представляют содержательную сторону информации.

---

[89] См.: ст.ст. 33, 76[1] УК РФ.
[90] См.: ст.ст. 138[1], 140, 144, 159[6], 171[1], 185, 185[1], 185[6], 187, 189, 193, 205[1], 237, 272, 273, 274, 274[1], 287 УК РФ.
[91] См.: ст.ст. 128[1], 137, 185[3], 205[2], 228[1], 242, 280, 280[1], 282, 354, 354[1] УК РФ.
[92] См.: ст.ст. 110[1], 110[2], 137, 159[6], 171[2], 185[3], 228[1], 242, 242[1], 242[2], 274, 280, 280[1], 282 УК РФ.
[93] См.: ст. 63[1] УК РФ
[94] См.: ст.ст. 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], 272, 275, 276, 283, 283[1], 284, 285[3], 292, 292[1], 311, 320, 354[1] УК РФ
[95] Ефремова Т. Ф. Новый словарь русского языка. Толково-словообразовательный. М.: Русский язык, 2000. URL: http://www.efremova.info/word/svedenija.html (дата обращения: 17.07.2017).
[96] См.: Маскаева А. М. Указ. соч. С. 7.
[97] См.: Юрченко И. А. Указ. соч. С. 28.
[98] Минбалеев А. В. К вопросу рассмотрения информации как юридической фикции // Вестник ЮУрГУ. Серия: Право. 2006. № 13 (68). С. 119.

Понятие «данные» применяется законодателем только при конструировании составов преступлений в Особенной части УК РФ (ст.ст. 170^1, 173^1, 173^2, 272 и 310 УК РФ). Под «данными» в литературе понимается информация, представленная в *формализованном* виде и *предназначенная для обработки ее техническими средствами*[99]. По мнению Ф. С. Воройского, данные – это «сведения, факты, показатели, выраженные как в числовой, так и любой другой форме». Он также отмечает, что для разделения понятий «информация» и «данные» Ассоциация стандартов Франции дает следующие определения: «Данные – факт, понятие или инструкции, представленные в условной форме, удобной для пересылки, интерпретации и обработки человеком или автоматизированными средствами; … данные – некоторый факт, то, на чем основан вывод или любая интеллектуальная система … компонентами данных являются цифры и символы естественного языка или их кодированное представление в виде строки двоичных битов»[100]. Ученые выделяют важные признаки данных, с помощью которых они становятся информацией: правильность отражения объектов описания[101], интерес для субъекта, новизна, сокращение степени неопределенности[102].

В литературе понятие «данные» рассматривается также в широком и в узком смыслах. В широком смысле – это сведения, имеющие значения для формулирования вывода или принятия решения[103]. В узком – это «информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека»[104].

В Общей части УК РФ (ст. 31 УК РФ) и при конструировании отдельных составов преступлений (ст.ст. 138, 185^5, 207, 272) используется и понятие «сообщение». Понятие «данные» в широком смысле имеет сходство с понятием «сообщение» (*существительного*), определяемое как «упорядоченная

---

[99] См.: Баранова Е. К. Основы информатики и защиты информации [Электронный ресурс] : Учеб. пособие / Е. К. Баранова. М.: РИОР : Инфра-М, 2013. С. 17; Маскаева А. М. Указ. соч. С. 8.
[100] Воройский Ф. С. Указ. соч. С. 12.
[101] См.: Маскаева А. М. Указ. соч. С. 9.
[102] См.: Воройский Ф. С. Там же.
[103] Минбалеев А. В. Там же.
[104] Минбалеев А. В. Там же.

последовательность символов, предназначенная для передачи информации»[105], либо «последовательность символов, имеющая свою систему, предназначенная для передачи той же информации»[106]. Е. П. Тавокин в качестве основного свойства сообщения отмечает «возможность снижения с его помощью неопределенности у получателя сообщения»[107]. На наш взгляд, понятие «данные» в широком смысле тождественно понятию «сведения».

Как известно, УК РФ 1996 г. разрабатывался наряду с Модельным Уголовным кодексом для государств-участников СНГ (далее – МУК СНГ)[108], который также содержит составы преступлений, схожие с исследуемыми в настоящей работе (ст.ст. 286-292 МУК СНГ). Изменениями, внесенными в МУК СНГ постановлением Межпарламентской Ассамблеей государств-участников СНГ от 27.11.2015 г. № 43-16 в анализируемые статьи с 286 по 292 МУК СНГ, понятие «компьютерная *информация*» заменена на понятие «компьютерные *данные*».

Таким образом, комплексный анализ уголовного законодательства и его понятийного аппарата позволяет прийти к следующим выводам:

1. Понятия «информация» упоминается в 19 статьях УК РФ, «сообщение» – 3, «сведения» – 37, «данные» – 5. Таким образом, наиболее распространенным в УК РФ среди анализируемых понятий (информация, сообщения, сведения, данные) является понятие «сведения».

2. Как минимум одно из 4 анализируемых понятий (информация, сообщения, сведения, данные) используется в 57 статьях УК РФ, в т.ч. из которых 3 статьи располагаются в Общей части УК РФ, 54 статьи – в Особенной части УК РФ. Это свидетельствует о «степени проникновения» информационных отношений в УК РФ и отдельно в каждый из разделов и глав уголовного

---

[105] Першиков В. И., Савинков В. М. Толковый словарь по информатике. М.: Финансы и статистика, 1995. С. 77.
[106] Там же.
[107] Тавокин Е. П. Указ. соч. С. 131.
[108] См.: Иванцова Н. В. Модельный Уголовный кодекс для государств участников СНГ и уголовное законодательство Российской Федерации: сравнительно-правовой аспект // Пробелы в российском законодательстве. 2011. № 6. URL: http://cyberleninka.ru/article/n/modelnyy-ugolovnyy-kodeks-dlya-gosudarstv-uchastnikov-sng-i-ugolovnoe-zakonodatelstvo-rossiyskoy-federatsii-sravnitelno-pravovoy (дата обращения: 13.02.2017); Модельный Уголовный кодекс стран-участников СНГ : принят на седьмом пленарном заседании Межпарламентской Ассамблеи государств участников Содружества Независимых Государств (постановление № 7-5 от 17.02.1996 г.) URL: http://docs.cntd.ru/document/901781490 (дата обращения: 17.07.17).

законодательства. Вместе с тем отсутствие одного из рассматриваемых понятий в уголовно-правовой норме вовсе не означает, что такое деяние не может быть совершено в информационно-телекоммуникационной сфере. В качестве такого примера можно привести описание деяния в ст. 146 УК РФ «Нарушение авторских и смежных прав». Кроме того, диспозиция может не содержать одного из четырех понятий, вместе с тем в качестве объективного признака может содержаться указание на совершение того или иного преступления с использованием средств массовой информации либо информационного-телекоммуникационных сетей (включая сеть Интернет).

3. В трех статьях УК РФ понятия «сведения» и «данные» используются совместно. Понятия «сообщения» и «сведения» используются также наряду друг с другом в одной статье УК РФ. В одной из статей УК РФ указываются одновременно все четыре рассматриваемых нами определения (информация, сообщения, сведения, данные).

Как нам представляется, анализируемые термины в рассмотренных уголовно-правовых нормах являются взаимозаменяемыми. Их нельзя отождествлять только в диспозиции ст. 138 УК РФ, в которой говорится о нарушении тайны сообщений граждан, где понятие «сообщение» имеет уникальную смысловую нагрузку.

Перечисленные положения позволяют сделать вывод о том, что законодателем нарушен *системный* подход в законодательной технике к конструировании уголовного законодательства. При отождествлении понятий «информация», «сведения», «сообщения», «данные» в ФЗ № 149-ФЗ в уголовном законе те же понятия используются бессистемно.

Наряду с понятием «информация» в уголовном законодательстве имеется указание на один из ее видов – «компьютерная информация». В качестве основного признака компьютерной информации в примечании к ст. 272 УК РФ указывается *на форму* информации – форму электрических сигналов. Компьютер, воспринимая информацию в любой из ее форм, с помощью устройства ввода информации (клавиатуры, мыши, микрофона, видеокамеры и др.) кодирует получаемую

информацию в электрические сигналы для дальнейшей ее обработки. Поэтому любую информацию можно представить в форме электрических сигналов посредством ее кодирования. Определять компьютерную информацию через форму ее представления предлагает, к примеру, А. В. Суслопаров[109].

Такой существующий законодательный подход к такому определению компьютерной информации является уязвимым и вызывает справедливую критику со стороны других ученых. Так, передача информации через оптоволоконный кабель, в основе которого лежит способ передачи информации с помощью света, не является по своей сущности электронной. Информация такую форму приобретает только непосредственно при ее обработке компьютером. Другим примером является передача информации посредством Wi-Fi технологий – радиосигналов, которые преобразуются оконечным оборудованием в электрические сигналы. На практике возможен незаконный перехват радио- и световых сигналов, не являющихся электронными сигналами в процессе их передачи. Компьютерная информация на магнитных носителях информации (напр., банковские расчетные карты), CD, DVD-дисках также не является информацией, представленной в форме электрических сигналов.

Приведенные примеры на практике не исчерпываются другими противоречиями. Как справедливо отмечает И. А. Клепицкий, законодательное определение компьютерной информации позволяет под таковой понимать даже информацию в мозге человека или животного[110]. У специалистов в сфере информационных технологий такое положение вызывает вопросы. Например, как информацию признавать представленной в форме электрических сигналов, если она обрабатывается, хранится и передается не в форме электрических сигналов, вопреки положению, изложенному в прим. 1 к ст. 272 УК РФ?

Уязвимость ее определения через форму обработки, хранения и передачи информации, на наш взгляд, остро проявит себя в течение нескольких лет. При обработке компьютерным устройством информации в форме электрических

---

[109] Суслопаров А. В. Указ. соч. С. 82.

[110] Качество уголовного закона: проблемы Особенной части: монография / отв. ред. А. И. Рарог. М.: Проспект, 2017. С. 295.

сигналов основную функцию исполняет база, на которой оно построено, его процессор. Процессоры сегодня конструируются на основе электронных чипов, однако новые научные открытия позволяют разрабатывать иные типологии процессоров. Например, процессоры, построенные на квантовых технологиях, чья работа не основывается исключительно на электрических сигналах. Учеными уже объявлено об успешном создании первого 51-кубитного квантового компьютера, являющегося по своей производительности одним из самых мощных в мире[111]. Квантовый компьютер по своей мощности во много раз превосходит существующие компьютеры, что при пробельности существующего законодательства может серьезно повлиять на безопасность всех информационных систем. Элементарным методом взлома компьютерных паролей (ключей) – с помощью их подбора (брутофорсный метод), – с использованием производительности квантового компьютера станет возможным получить неправомерный доступ к компьютерной информации, находящейся на любой компьютерной технике, защищенной одним текстовым паролем. Столкнувшись с некоторыми из указанных противоречий, М. В. Старичков пришел к выводу, что основным признаком такой информации выступает предназначенность информации специально для обработки в компьютерных устройствах, а не ее форма представления[112].

Таким образом, в отечественной науке имеется два основных подхода к определению компьютерной информации: через *способ обработки указанной информации* и через *форму ее представления*.

Следует отметить, что в уголовном законодательстве «компьютерная информация» не всегда определялась через форму ее представления. Соответствующие изменения были внесены в прим. 1 ст. 272 только Федеральным законом № 420-ФЗ[113]. До их внесения под компьютерной информацией понималась

---

[111] См.: Физики из России и США создали первый 51-кубитный квантовый компьютер // Сетевое издание «РИА Новости». URL: https://ria.ru/science/20170714/1498476410.html (дата обращения: 26.07.17).

[112] См.: Старичков М. В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики: автореф. дис. … канд. юрид. наук. Иркутск, 2006. С. 19-20.

[113] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации : федер. закон Рос. Федерации от 7 дек. 2011 г. № 420-ФЗ // Собр. законодательства Рос. Федерации. 2011. № 50, ст. 7362.

«информация на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети». То есть законодатель уклонился от понимания компьютерной информации через способ ее передачи и обработки.

На наш взгляд, в Соглашении о сотрудничестве стран СНГ в борьбе с преступлениями в сфере компьютерной информации используется весьма удачный смешанный подход к определению компьютерной информации как через форму, так и через способ обработки компьютерной информации. В нем указывается, что под ней следует понимать информацию, находящуюся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи[114].

Основным признаком компьютерной информации является возможность произведения над ней различных операций компьютерными техническими средствами. Под возможностью воспроизведения операций над сведениями понимается возможность ее распространения, сбора, обработки, хранения, предоставления и поиска. Поэтому мы считаем, что понятие компьютерной информации следует раскрывать как через *способ* ее обработки, так и через ее *форму*. Под компьютерной информацией следует понимать сведения, представленные в оперируемой техническими средствами форме.

Указанное понятие, на наш взгляд, необходимо изложить в пункте 1.1 статьи 2 ФЗ № 149-ФЗ наряду с такими понятиями, как «информация», «информационные технологии», «информационная система», «информационно-телекоммуникационная сеть» и др. Такие понятия следует излагать в специальном законодательстве, а соответствующие диспозиции норм уголовного законодательства станут бланкетными. Это позволит уголовному закону более гибко реагировать на процессы совершенствования компьютерной техники. Однако следует отметить, что концепция указанного федерального закона строится на таком же понимании компьютерной информации, как и в нынешнем

---

[114] Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г., г. Минск // Справочно-правовая система Гарант. URL: http://garant.ru (дата обращения: 17.07.17).

уголовном законодательстве[115]. Поэтому предлагаемые нами изменения должны повлечь системное изменение понятийного аппарата, изложенного в ФЗ № 149-ФЗ.

В новой уголовно-правовой норме о противодействии неправомерному воздействию на КИИ РФ указывается на компьютерную информацию, содержащуюся в КИИ РФ. Таким образом, она предопределяет новый подход к классификации компьютерной информации, в которой следует отграничивать компьютерную информацию *общего* характера от содержащейся в КИИ РФ.

В литературе встречается широкое и узкое понимания преступлений в сфере компьютерной информации. В широком смысле под преступлениями в сфере компьютерной информации понимаются преступления, в котором компьютер используется в качестве средства или орудия совершения преступления[116]. Однако, в таком случае, на наш взгляд, мы должны говорить о компьютерных преступлениях, но не о преступлениях в сфере компьютерной информации. В узком смысле под преступлениями в сфере компьютерной информации понимаются преступления, в которых указанная информация является предметом посягательства [117] . Это фактически те преступления, которые невозможно совершить без использования компьютера. Ответственность за их совершение предусмотрена статьями 272 УК РФ (неправомерный доступ к компьютерной информации), 273 УК РФ (создание, использование и распространение вредоносных компьютерных программ), 274 УК РФ (нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей) и 274^1 УК РФ (неправомерное воздействие на КИИ РФ), расположенные в гл. 28 УК РФ «Преступления в сфере компьютерной информации». К ним также следует отнести и мошенничество в сфере компьютерной информации (ст. 159^6 УК РФ), в котором дополнительным объектом уголовно-правовой охраны является также

---

[115] См. изложенные в нем понятия «электронного документа», «электронного сообщения» и др.

[116] См.: Толеубекова Б. Х. Компьютерная преступность: уголовно-правовые и процессуальные аспекты. Караганда, КВШ МВД СССО, 1991. С. 35-36.

[117] См.: Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления / Законность. 1997. № 1. С. 9.

компьютерная информация и само преступление не может быть совершено без использования компьютерной техники.

Таким образом, более приемлемым в целом представляется имеющийся подход к разграничению «преступлений в сфере компьютерной информации» и «компьютерных преступлений» по тем же критериям[118].

М. В. Старичков определяет *преступления в сфере компьютерной информации* как запрещенные УК РФ под угрозой наказания виновно совершенные общественно опасные деяния, посягающие на общественные отношения, связанные с правомерным и безопасным использованием охраняемой законом информации ЭВМ [119] . М. Ю. Дворецкий под ними понимает «предусмотренные уголовным законом виновные общественно опасные деяния, *направленные* на нарушение *неприкосновенности* (курсив наш – Р. Г.) охраняемой законом компьютерной информации и ее материальных носителей, совершаемые в процессе создания, использование и распространение компьютерной информации и информационных ресурсов, а также эксплуатации систем обработки информации с использованием ЭВМ, систем ЭВМ или их сетей, причиняющие или создающие угрозу причинения вреда законным интересам собственников или владельцев, жизни и здоровью личности, правам и свободам человека и гражданина, государственной и общественной безопасности»[120]. В свою очередь, М. А. Зубова их определяет как «виновно совершенные общественно опасные деяния, *посягающие* на нормальный *порядок обращения* (курсив наш – Р. Г.) охраняемой законом компьютерной информации, запрещенные УК РФ под угрозой наказания» [121] . Е. В. Лошенкова в качестве таких преступлений понимает «предусмотренные уголовным законом общественно опасные деяния, причиняющие вред или создающие опасность причинения вреда безопасности

---

[118] См.: Вехов В. Б. Компьютерные преступления: Способы совершения и раскрытия. М.: Право и Закон, 1996. С. 23.
[119] См.: Старичков М. В. Указ. соч. С. 13.
[120] Дворецкий М. Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания: Монография. Тамбов, 2003. С. 13.
[121] Зубова М. А. Указ. соч. С.10.

производства, хранения, использования либо распространения информации или информационных ресурсов»[122].

На наш взгляд, наиболее полно сущностную характеристику отражает формулировка рассматриваемых преступлений 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 КИИ РФ.

В указанном определении словосочетание «в сфере» не случайно заменено другим – «против безопасности». Такая необходимость обусловливается системной структурой Особенной части УК РФ, в котором все посягательства на видовые объекты (за исключением двух) определены через термин «против». Более того, безопасность компьютерной информации является конкретно определенным объектом уголовно-правовой охраны в отличие от всеобъемлющего понятия «сфера». Одно из значений термина «сфера» – область, пределы чего-либо, круг деятельности[123]. Преступное же деяние всегда посягает на конкретный объект преступления, который должен быть закреплен в качестве объекта уголовно-правовой охраны. В предлагаемом нами определении конкретизируются видовые и непосредственные объекты уголовно-правовой охраны и преступления, содержание которых будет нами раскрыто в § 1 главы 3 настоящей работы.

Таким образом, понятие компьютерных преступлений является более широким понятием по сравнению с преступлениями в сфере компьютерной информации и включает их в себя. Такой подход, имеющийся в теории уголовного права, к разграничению компьютерных преступлений и преступлений в сфере компьютерной информации не вызывает сомнений[124]. Уточняя его, отметим, что

---

[122] Российское уголовное право. Особенная часть: Учебник / Под ред. А. И. Чучаева. М.: НИЦ Инфра-М: КОНТРАКТ, 2012. С. 300.

[123] См.: Толковый словарь русского языка под ред. С.И. Ожегова и Н.Ю. Шведовой. М., 1997. URL: http://dic.academic.ru/dic.nsf/ogegova/237222 (дата обращения 17.07.17).

[124] См. подробнее: Зинина У. В. Указ. соч. С. 36; Копырюлин А. Н. Преступления в сфере компьютерной информации: уголовно-правовой и криминологический аспекты : дис. … канд. юрид. наук. Тамбов, 2007. С. 35;

основным, дополнительным либо факультативным объектом посягательства при совершении компьютерных преступлений будет выступать компьютерная безопасность, т.е. состояние защищенности компьютерных и сетевых устройств от угроз различного характера.

§ 2. Проблемы криминализации посягательств на безопасность компьютерной информации: сравнительно-правовой аспект

Впервые уголовная ответственность за рассматриваемые преступления нашла свое отражение в главе 28 УК РФ 1996 г. Такое положение не означает, что преступлений против безопасности компьютерной информации и компьютерной преступности не существовало как социальных явлений. Введение уголовной ответственности за неправомерные деяния в рассматриваемой сфере было обусловлено научно-технической революцией, последующим за ней информационно-технологическим перевооружением предприятий и учреждений, появлением мирового информационного пространства[125]. Такие деяния ранее могли квалифицироваться правоприменителем, например, по ст. 98 УК РСФСР[126].

В последующем в главу 28 УК РФ неоднократно вносились изменения, которые в основном касались установленных санкций за совершения соответствующих преступлений[127]. Федеральный закон № 420-ФЗ внес

Зубова М. А. Компьютерная информация как объект уголовно-правовой охраны: дис. … канд. юрид. наук. Казань, 2008. С. 53.

[125] См.: Преступления в сфере компьютерной информации: квалификация и доказывание. Учебное пособие / Гаврилин Ю.В., Головин Ю. В., Кузнецов А. В., Толстухина Т. В. М.: Книжный мир, 2003. С. 5.

[126] как умышленное уничтожение или повреждение государственного или общественного имущества, умышленное уничтожение носителей с машинной информацией, уничтожение (удаление) файлов. Подробнее см.: Батурин Ю. М. Жодзишский А. М. Указ. соч. С. 24.

[127] О внесении изменений и дополнений в Уголовный кодекс Российской Федерации : федер. закон Рос. Федерации от 8 дек. 2003 г. № 162-ФЗ : принят Гос. Думой Федер. Собр. Рос. Федерации 21 нояб. 2003 г. : одобр. Советом Федерации Федер. Собр. Рос. Федерации 26 нояб. 2003 г. // Собрание законодательства РФ. 2003. № 50, ст. 4848; О внесении изменений в Уголовный кодекс Российской Федерации в части назначения наказания в виде обязательных работ : федер. закон от 6 мая 2010 г. № 81-ФЗ : принят Гос. Думой Федер. Собр. Рос. Федерации 23 апр. 2010 г. : одобр. Советом Федерации Федер. Собр. Рос. Федерации 28 апр. 2010 г. // Собрание законодательства РФ. 2010. № 19, ст. 2289; О внесении изменений в Уголовный кодекс Российской Федерации : федер. закон от 7 марта 2011 г. № 26-ФЗ : принят Гос. Думой Федер. Собр. Рос. Федерации 25 фев. 2011 г. : одобр. Советом Федерации Федер. Собр. Рос. Федерации 2 марта 2011 г. // Собрание законодательства РФ. 2011. № 11, ст. 1495; О внесении изменения в статью 272 Уголовного кодекса Российской Федерации : федер. закон от 28 июня 2014 г. № 195-ФЗ : принят Гос. Думой Федер. Собр. Рос. Федерации 18 июня 2014 г. : одобр. Советом Федерации Федер. Собр. Рос. Федерации 25 июня 2014 г. // Собрание законодательства РФ. 2014. № 26 (часть I), ст. 3401.

существенные изменения касаемо понятийного аппарата рассматриваемых преступлений. ФЗ № 194-ФЗ глава 28 УК РФ дополнена с 01.01.2018 г. новым составом, устанавливающим ответственность за неправомерное воздействие на КИИ РФ (ст. 274[1] УК РФ). Однако внесенные изменения обострили имеющиеся противоречия в конструкциях таких составов. Вместе с тем ФЗ № 194-ФЗ необходимо усиливает уголовную ответственность за посягательства на государственные информационные объекты, представляющие угрозу национальной безопасности страны.

Особое внимание борьбе с компьютерной преступностью уделяется на международном уровне, о чем свидетельствуют регулярно проводимые международные научно-практические форумы и заседания [128], посвященные узкоспециализированной тематике, принятие международных соглашений, направленных на борьбу с компьютерными преступлениями [129], создание на межгосударственном и государственном уровне специализированных органов по борьбе с компьютерной преступностью[130].

Если ранее в мире признавались три основных подхода к криминализации компьютерных правонарушений, в сущности различающихся по объекту уголовно-правовой охраны: криминализация несанкционированного доступа в защищенные компьютерные системы, заражения вирусами, и т.д.; признания компьютерными преступлениями только деяний, связанных с причинением ущерба имуществу и электронной обработке информации; криминализация деяний, связанных с причинением имущественного ущерба, а также с нарушением прав личности, угрозой национальной безопасности и т.д. Сегодня мы можем говорить о тенденции к признанию в качестве компьютерных преступлений двух основных ее видов: высокотехнологичных преступлений и преступлений,

---

[128] К примеру, 4th INTERPOL-Europol Cybercrime Conference (28-30 Сентября 2016, Сингапур); IFIP SEC 2016 Gent, Belgium; INTERNATIONAL CONFERENCE O№ CYBER SECURITY, JULY 25 28, 2016; Third Annual Journal of Law and Cyber Warfare Conference № November 2016; The Law and Policy of Cybersecurity, February 5, 2016 | Rockville, Maryland, USA и др.

[129] Напр., Конвенция Совета Европы о преступности в сфере компьютерной информации : ETS № 185, 23.11.2001, Будапешт; п. «h» ч. 1 Конвенции ООН против транснациональной организованной преступности : принята резолюцией 55/25 Генеральной Ассамблеи от 15 ноября 2000 года; Создание глобальной культуры кибербезопасности : Резолюция, принята Генеральной Ассамблеей 31.01.2003.

[130] Напр., Cyber Division at FBI Headquarters USA, Управление «К» БСТМ МВД России, Интерпол.

связанных с компьютерной инфраструктурой. Иными словами, под первыми понимаются виды преступлений, которые могут быть совершены только посредством использования компьютерной техники (преступлений против безопасности компьютерной информации), под последними – «традиционные» преступления, которые могут совершаться в т.ч и посредством компьютерной техники (компьютерные преступления).

Уголовными законами зарубежных стран также предусматривается ответственность за различные посягательства на безопасность компьютерной информации. Сравнительно-правовой метод изучения уголовного законодательства зарубежных государств предполагает их анализ в системе. В качестве такой системы нами предлагается рассмотрение стран участников Содружества Независимых Государств (далее – СНГ), в том числе ранее входивших в СНГ, и наиболее развитых европейских стран. Круг стран - участников СНГ в нашем исследовании ограничен странами с наиболее высоким уровнем ВВП на душу населения – это Казахстан, Белоруссия, Грузия, Армения, Узбекистан и Украина[131]. Также представляется необходимым для анализа выбрать наиболее развитые европейские страны со схожей отечественной правовой системой – романо-германской правовой семье. Общеизвестно, что наиболее активно компьютерная преступность проявляется в странах с развитой экономикой и прорывными технологиями. Среди таких стран мы можем отметить Федеративную Республику Германия (далее – ФРГ) и Французскую Республику.

Система уголовных кодексов стран, входящих (в т.ч. ранее) в СНГ, построена на едином Модельном Уголовном кодексе стран СНГ, чем объясняется схожесть архитектоники уголовных кодексов с УК РФ, в том числе основных институтов уголовного права: понятия преступления, видов преступлений, видов применяемых наказаний и их размеров и др., и поэтому они упущены нами при рассмотрении уголовного законодательства стран-участников СНГ ввиду их

[131] Приведены в порядке убывания по данным Всемирного Банка по состоянию на 2015 г., опубликовано 01 июля 2016 г. URL: http://data.worldbank.org/indicator/NY.GDP.PCAP.CD (дата обращения: 27.07.17); Данные по Республике Беларусь приведены из иных открытых источников в связи с отсутствием в списке Всемирного Банка. URL: https://myfin.by/info/valovoj-vnutrennij-produkt (дата обращения: 27.07.17).

схожести с уголовным законодательством Российской Федерации[132]. И напротив, названные институты проанализированы при сравнительно-правовом анализе уголовного законодательства ФРГ и Французской Республики.

Уголовный кодекс Республики Казахстан (далее – УК РК) представляет собой интерес как наиболее «молодой» среди всех рассматриваемых кодифицированных актов. В УК РК предусматривается деление Особенной части только на главы, без объединения их в разделы[133]. Схожие отечественным составам преступлений против безопасности компьютерной информации составы расположены в Главе 7 «Уголовные правонарушения в сфере информатизации и связи» УК РК [134] . Объектом рассматриваемых преступлений, как указывает законодатель, являются общественные отношения в сфере информатизации и связи.

Составами преступлений, не известными отечественному правоприменителю, и некоторым образом, устраняющими пробельность российского уголовного законодательства, являются ст.ст. 209, 212 и 213 УК РК. Другие составы – ст.ст. 205, 206, 208, 211 УК РК – схожи с признаками отечественной конструкции, предусмотренной ст. 272 УК РФ; деяния, ответственность за которые предусмотрена ст. 210 УК РК, – ст. 273 УК РФ, а конструкция состава преступления ст. 207 УК РК по своим признакам схожа со ст. 274 УК РФ.

В уголовном законодательстве РК наблюдается достаточно эффективная дифференциация уголовных правонарушений. Среди перечисленных составов

---

[132] Положение о разработке модельных законодательных актов и рекомендаций Межпарламентской Ассамблеи государств-участников Содружества Независимых Государств : Принято в г. Санкт-Петербурге 14 апр. 2005 г. Постановлением 25-8 на 25-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ : с изм. и доп. от 25 нояб. 2008 г.

[133] Уголовный кодекс Республики Казахстан от 3 июля 2014 года №226-V ЗРК // URL: https://online.zakon.kz/Document/?doc_id=31575252#pos=2375;-316 (дата обращения: 18.07.17).

[134] Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций (ст. 205), неправомерные уничтожение или модификацию информации (ст. 206), нарушение работы информационной системы или сетей телекоммуникаций (ст. 207), неправомерное завладение информацией (ст. 208), принуждение к передаче информации (ст. 209), создание, использование или распространение вредоносных компьютерных программ и программных продуктов (ст. 210), неправомерное распространение электронных информационных ресурсов ограниченного доступа (ст. 211), предоставление услуг для размещения Интернет-ресурсов, преследующих противоправные цели (ст. 212), неправомерные изменения идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства (ст. 213).

преступлений в качестве уголовных проступков признаются ч.ч. 1 и 2 ст. 205, ч. 1 ст. 206, ч. 1 ст. 208, ч. 1 ст. 211, ч. 1 ст. 213 УК РК. Следовательно, за их совершение не предусмотрено наказание в виде лишения свободы.

Составы преступлений, предусматривающие ответственность за уголовные правонарушения в сфере информатизации и связи, содержат квалифицирующий признак – «деяние, совершенное в отношении государственных электронных информационных ресурсов или информационных систем государственных органов». Такое положение нам представляется весьма приемлемым для имплементации в отечественное законодательство, однако она решена отечественным законодателем иным образом, путем введения в гл. 28 УК РФ нового состава преступления – ст. 274[1] УК РФ.

В Уголовном кодексе Республики Беларусь (далее – УК РБ) составы, регламентирующие ответственность за рассматриваемые нами преступления, расположены в Главе 31 «Преступления против информационной безопасности» Раздела XII «Преступления против информационной безопасности» [135] . Информационная безопасность в уголовном законодательстве Республики Беларусь выделяется в качестве самостоятельного родового объекта уголовно-правовой охраны наряду с общественным порядком и общественной нравственностью (Гл. XI УК РБ). Объект преступлений против информационной безопасности является более широким объектом уголовно-правовой охраны, в отличие от объекта преступлений против безопасности компьютерной информации. Принципиально отличающихся конструкций от составов преступлений, расположенных в гл. 28 УК РФ, в УК РБ не содержится[136].

Все составы преступлений против информационной безопасности за исключением ст.ст. 352 (неправомерное завладение компьютерной информацией)

---

[135] Уголовный кодекс Республики Беларусь от 9 июля 1999 года №275-З // URL: http://www.base.spinform.ru/show_doc.fwx?rgn=1977 (дата обращения: 18.07.17).

[136] В Главе 31 УК РБ регламентирована ответственность за несанкционированный доступ к компьютерной информации (ст. 349), модификацию компьютерной информации (ст. 350), компьютерный саботаж (ст. 351), неправомерное завладение компьютерной информацией (ст. 352), изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети (ст. 353), разработка, использование либо распространение вредоносных программ (ст. 354) и нарушение правил эксплуатации компьютерной системы или сети (ст. 355).

и 353 (изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети) УК РБ предусматривают ответственность за квалифицированные виды преступлений.

Статьи 349, 350 и 354 УК РБ по своим конструктивным признакам близки составу преступления, ответственность за которое предусматривается ст. 272 УК РФ, но в расчлененном виде. Статья 354 УК РБ по своим признакам схожа со ст. 273 УК РФ. Статья 355 УК РБ – со статьей 274 УК РФ. Неизвестным составом преступления для российского правоприменителя является только состав ст. 351 УК РБ (компьютерный саботаж).

Уголовный кодекс Грузии (далее – УК Грузии) [137] предусматривает ответственность за киберпреступления в Главе XXXV девятого раздела «Преступления против общественной безопасности и общественного порядка»[138]. По своему смыслу деяния, ответственность за которые предусмотрена ст.ст. 284 и 286, могут квалифицироваться в отечественной практике по ст. 272 УК РФ. Деяние, ответственность за которые регламентирована ст. 285 УК Грузии, схожа с деянием, ответственность за которое предусмотрена ст. 273 УК РФ. Неизвестным составом преступления для грузинского правоприменителя является отечественная норма – ст. 274 УК РФ, вместе с тем возможность квалификации такого деяния по совокупности с иными составами преступлениями УК Грузии не исключает.

В Уголовном кодексе Республики Армения (далее – УК РА) [139] схожие отечественным составам рассматриваемых преступлений содержатся в Главе 24 «Преступления против безопасности компьютерной информации», расположенной в Разделе 9 «Преступления против общественной безопасности, безопасности компьютерной информации, общественного порядка, общественной нравственности и здоровья населения»[140].

---

[137] Уголовный кодекс Грузии от 13.08.1999 г. № 41 (48) // URL: https://matsne.gov.ge/ka/document/view/16426, https://matsne.gov.ge/ka/document/download/16426/143/ru/pdf (дата обращения: 18.07.17).

[138] Самовольное проникновение в компьютерную систему (ст. 284), незаконное использование компьютерных данных или (и) компьютерных систем (ст. 285) и посягательство на компьютерные данные или (и) компьютерную систему (ст. 286).

[139] Уголовный кодекс Республики Армения от 18.04.2003 г. // URL: http://www.parliament.am/legislation.php?sel=show&ID=1349&lang=rus (дата обращения: 18.07.17).

[140] Несанкционированный доступ (проникновение) к системе компьютерной информации (ст. 251), изменение компьютерной информации (ст. 252), компьютерный саботаж (ст. 253), неправомерное завладение компьютерной

Статья 272 УК РФ по своим элементам наиболее схожа с составами преступлений, расположенными в ст.ст. 251 и 252 УК РА. Состав преступления ст. 273 УК РФ – ст. 256 УК РА. Статья 274 УК РФ – ст. 257 УК РА. Неизвестными отечественному правоприменителю остается состав преступления, предусматривающий ответственность за компьютерный саботаж (ст. 253 УК РА).

Уголовный кодекс Республики Узбекистан (далее – УК РУ)[141] содержит группу близких к отечественным составам преступлений против безопасности компьютерной информации в Главе XX[1] «Преступления в сфере информационных технологий», расположенной в Разделе шестом «Преступления против общественной безопасности и общественного порядка»[142].

Таким образом, ст. 272 УК РФ по описательной части соответствуют ст.ст. 278[2], 278[4] УК РУ, ст. 273 УК РФ – ст. 278[6] УК РУ, ст. 274 УК РФ – ст. 278[1] УК РУ. Неизвестные отечественному законодательству составами преступлений являются компьютерный саботаж (ст. 278[5] УК РУ) и изготовление с целью сбыта либо сбыт и распространение специальных средств для получения незаконного (несанкционированного) доступа к компьютерной системе (ст. 278-3 УК РУ).

Уголовный кодекс Украины (далее – УК Украины) делится на части (Общая и Особенная) и разделы, деления на главы в структуре кодекса не предусматривается[143]. Наиболее схожим разделом в УК Украины отечественной главе 28 УК РФ является Раздел XVI «Преступления в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей

информацией (ст. 254), изготовление или сбыт специальных средств неправомерного доступа (проникновения) к компьютерной информации (ст. 255), разработка, использование и распространение вредоносных программ (ст. 256), нарушение правил эксплуатации компьютерной системы или сети (ст. 257).

[141] Уголовный кодекс Республики Узбекистан от 22 сент. 1994 г. // URL: http://lex.uz/pages/getpage.aspx?lact_id=111457 (дата обращения: 17.07.17).

[142] Нарушение правил информатизации (ст. 278-1), незаконный (несанкционированный) доступ к компьютерной информации (ст. 278-2), изготовление с целью сбыта либо сбыт и распространение специальных средств для получения незаконного (несанкционированного) доступа к компьютерной системе (ст. 278-3), модификация компьютерной информации (ст. 278-4), компьютерный саботаж (ст. 278-5), создание, использование или распространение вредоносных программ (ст. 278-6).

[143] Уголовный кодекс Украины от 5 апр. 2001 г. № 2341-III // СоюзПравоИнформ. URL: http://zakon5.rada.gov.ua/laws/2341-14 (дата обращения: 17.07.17).

и сетей электросвязи» в котором и сгруппированы соответствующие составы преступлений[144].

Видовым объектом рассматриваемых составов преступлений является правомерность использования компьютеров, систем и компьютерных сетей и сетей электросвязи. В наиболее общем виде рассматриваемые составы преступлений в УК Украины можно соотнести с составами преступлений, расположенными в УК РФ. Так, деяния, ответственность за которые предусматривается ст.ст. 361, 361^2, 362, 363^1 по конструктивным признакам близки к ст. 272 УК РФ, ст. 361^1 – схожа со ст. 273 УК РФ, а ст. 363 УК Украины – со ст. 274 УК РФ.

Таким образом, во всех уголовных кодексах стран СНГ содержатся составы преступлений, во многом схожие с составами преступлений, имеющимися в отечественном законодательстве. Некоторые страны-участники СНГ за постсоветский период развития уголовного законодательства внесли существенные изменения в сфере регламентации уголовной ответственности рассматриваемых деяний.

Некоторые страны-участники СНГ в отличие от Российской Федерации включили в уголовное законодательство составы компьютерного саботажа (напр., ст. 253 УК РБ, ст. 351 УК РА) и изготовления и сбыта специальных средств для получения неправомерного доступа к компьютерной системе или сети (напр., ст. 353 УК РБ, ст. 255 УК РА, ст. 278-3 УК РУ, ст. 361^1 УК Украины). Следует сказать, что похожий на последний состав преступления был впоследствии включен в 2011 г. в УК РФ в виде ответственности за незаконный оборот специальных технических средств, предназначенных для негласного получения информации (ст. 138^1 УК РФ)

---

[144] Несанкционированное вмешательство в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи (ст. 361), создание в целях использования, распространения или сбыта вредных программных или технических средств, а также их распространение или сбыт (ст. 361^1), несанкционированные сбыт или распространение информации с ограниченным доступом, хранящейся в электронно-вычислительных машинах (компьютерах), автоматизированных системах, компьютерных сетях или на носителях такой информации (ст. 361^2), несанкционированные действия с информацией, которая обрабатывается в электронно-вычислительных машинах (компьютерах), автоматизированных системах, компьютерных сетях или хранится на носителях такой информации, совершенные лицом, имеющим право доступа к ней (ст. 362), нарушение правил эксплуатации электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи либо порядка или правил защиты информации, которая в них обрабатывается (ст. 363) и воспрепятствование работе электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи путем массового распространения сообщений электросвязи (ст. 363^1).

в Главу 19 «Преступления против конституционных прав и свобод человека и гражданина» [145] . Следует также отметить, что изменилось законодательство Казахстана в части введения уголовной ответственности за посягательства на государственную информационную структуру.

Анализируя содержащиеся санкции, предусмотренные уголовно-правовыми нормами стран-участников СНГ за преступления против безопасности компьютерной информации, отметим, что существенной разницы они не содержат, в каких-то проанализированных странах ответственность является мягче (например, в Грузии, Армении, Узбекистане), а в других несущественно выше (это Казахстан, Беларусь, Украина).

В целях возможной последующей имплементации в отечественное уголовное законодательство представляют интерес положения ст.ст. 212 УК РК (предоставление услуг для размещения Интернет-ресурсов, преследующих противоправные цели), 213 УК РК (неправомерные изменения идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства), 363^1 УК Украины (воспрепятствование работе электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи путем массового распространения сообщений электросвязи) и 361^2 УК Украины (несанкционированные сбыт или распространение информации с ограниченным доступом, хранящейся в электронно-вычислительных машинах (компьютерах), автоматизированных системах, компьютерных сетях или на носителях такой информации).

Кроме того, в некоторых уголовных кодексах законодателем пересмотрен подход к наименованию глав, в которых содержатся составы преступлений, предусматривающие ответственность за рассматриваемые деяния. Соответствующая глава УК РК сейчас именуется «Уголовные правонарушения в

---

[145] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации : Федеральный закон от 7 дек. 2011 г. № 420-ФЗ // Собр. законодательства Рос. Федерации. 2011. № 50, ст. 7362.

сфере информатизации и связи», а ранее – «Преступления против безопасности информационных технологий» (в УК РК 1997 г.).

Уголовное законодательство Федеративной Республики Германии состоит из Основного закона (Конституции) ФРГ 1949 г., Уголовного уложения (Уголовного кодекса) ФРГ 1871 г. (далее – УУ ФРГ), федеральных уголовных законов, уголовного законодательства земель и иностранного уголовного законодательства [146]. В качестве основных видов наказаний УУ ФРГ предусматривает денежный штраф (§ 40) и пожизненное или временное лишение свободы (§ 38). Дополнительным видом наказания является запрет управления транспортным средством (§ 44).

УУ ФРГ признает уголовно наказуемыми преступные посягательства с использованием компьютерной техники. Специальный раздел о преступлениях против безопасности компьютерной информации в УУ ФРГ отсутствует[147]. В немецком уголовном законе схожие преступления по объекту уголовно-правовой охраны находятся в двух разделах УУ ФРГ – это Пятнадцатый раздел «Нарушение неприкосновенности частной жизни и частных тайн» (§§ 202a, 202b, 202c) и Двадцать седьмой раздел «Общеопасные преступные деяния» (§§ 303a, 303b).

В немецкой уголовно-правовой доктрине также имеется две основные точки зрения понимания компьютерных преступлений, согласно которым в узком смысле под ними понимаются все преступления, совершение которых представляется возможным только посредством компьютерной техники (§§ 202a, 202b, 202c, 303a, 303b), а в широком – традиционные преступления, или иными словами перенесенные из реальной жизни в виртуальную [148]. В качестве компьютерных преступлений, совершение которых представляется возможным только посредством компьютерной техники, являются следующие составы преступлений в УУ ФРГ: выведывание данных (§202a), перехват данных (§202b),

---

[146] Уголовное право зарубежных стран. Общая и Особенная части : учебник для магистров / под ред. Н. Е. Крыловой. 4-е изд., перераб. и доп. М.: Юрайт, 2015. С. 407.

[147] См. подробнее: Головненков П. В. Уголовное уложение (Уголовный кодекс) Федеративной Республики Германия. 2-е изд., перераб. и доп. М.: Проспект, 2014. С. 24.

[148] См.: Головненков П. Компьютерная преступность в Германии и система деликтов // Преступления в сфере экономики: российский и европейский опыт: материалы VI совместного российско-германского круглого стола, Москва, 23 октября 2014 г. / ред. кол.: А. И. Рарог, Т. Г. Понятовская. М., 2015. С. 28-29.

подготовка к выведыванию и перехвату данных (§202c), расположенные в XV разделе «Нарушение неприкосновенности частной жизни и частных тайн»; изменение данных (§303a) и компьютерный саботаж (§303b), расположенные в XXVII разделе «Повреждение вещей».

К другим компьютерным преступлениям в широком смысле можно отнести следующие составы преступлений: нарушение конфиденциальности слова, особо личной области частной жизни посредством съемки изображений, тайны переписки, частных тайн, почтовой и телекоммуникационной тайны, использование чужих тайн (§§ 201, 201a, 202, 203, 204, 206), расположенные в XV разделе «Нарушение неприкосновенности частной жизни и частных тайн»; подделку технических записей (§268), подделку значимых для доказывания данных (§269, §270), сокрытие документов (§274), расположенные в XXIII разделе «Подделка документов»; создание помехи для работы телекоммуникационных установок (§317), расположенное в XXVIII разделе «Общеопасные преступные деяния»; мошенничество (§263), компьютерное мошенничество (§263a), злоупотребление чековыми и кредитными картами (§266b), расположенные в XXII разделе «Мошенничество и злоупотребление доверием»; и другие преступления, расположенные в других разделах Особенной части УУ ФРГ, напр., распространение порнографических материалов (§§ 184 и след.), материалов, демонстрирующих насилие (§ 131), оскорбление (§§ 184 и след.), неправомерное преследование (§ 238) и пр., а также в «дополнительном уголовном праве», например, нарушение неприкосновенности тайной информации (§§ 3, 43, 44 Закона ФРГ о защите личных данных, Закона ФРГ о противодействии недобросовестной конкуренции), неправомерное прослушивание (§§ 89, 148 Закона ФРГ о телекоммуникации), нарушение авторских прав (§§ 106, 108, 108b Закона ФРГ о защите авторских прав) и пр.[149]

[149] См.: Головненков П. Указ. соч. С. 34; Weisser B. Cyber Crime. The information Society and Related Crimes. Section № 2. Special Part. National Report o№ Germany // Electronic Review of the International Association of Penal Law. Preparatory Colloquium Section II. Moscow (Russia), 24-27 April, 2013. Criminal Law. Special Part // URL: http://www.penal.org/sites/default/files/files/RM-8.pdf (дата обращения: 17.07.17).

В связи с ратификацией ФРГ Конвенции Совета Европы преступным деянием признано компьютерное мошенничество (§263а УУ ФРГ). Поскольку указанные в § 263а УУ ФРГ [150] формы реализации объективной стороны выступают в качестве способов достижения корыстной цели, субъектом преступления компьютер используется как средство совершения преступления[151]. УУ ФРГ не связывает компьютерное мошенничество с изъятием и (или) обращением имущества. Достаточным признаком является нанесение ущерба.

Уголовному законодательству Германии также знаком институт множественности преступлений. В соответствии с §53 УУ ФРГ возможна квалификация преступных деяний с использованием компьютерной техники по совокупности с другими преступлениями. Вместе с тем УУ ФРГ такие деяния полностью охватываются составом преступления §263а (компьютерное мошенничество), что придает конструктивную законченность норме, в отличие от состава преступления, предусмотренного ст. 159^6 УК РФ.

Примечательно, что немецким законодательством под данными понимаются такие, которые хранятся или передаются электронным, магнитным или иным *непосредственно не воспринимаемым человеком* способами. Таким образом, в УУ ФРГ иной, более совершенный подход к определению компьютерной информации в отличие от отечественного законодательства.

Нормой о компьютерном саботаже (§ 303b) предусматривается ответственность за значительное нарушение обработки данных, имеющих существенное значение для другого лица. Квалифицирующим признаком компьютерного саботажа является наличие особого объекта посягательства – существенного значения обработки данных для чужого предприятия, корпорации или государственного органа (абз. 2 § 303b).

---

[150] Уголовное уложение Федеративной Республики Германия // URL: http://www.gesetze-im-internet.de/bundesrecht/stgb/gesamt.pdf (дата обращения: 17.07.17).

[151] См.: Хилюта В. В. Уголовная ответственность за хищения с использованием компьютерной техники // Журнал российского права. 2014 № 3 (207) С. 114; Орловская Н. А. Зарубежный опыт противодействия компьютерной преступности (проблемы криминализации и наказуемости) // Сборник научных трудов международной конференции «Информационные технологии и безопасность». Вып. 1. Киев, 2003. С. 110-118.

В УУ ФРГ отсутствует выделение создания, использования и распространения ВКП, нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей в качестве отдельных составов преступлений. Такие действия могут образовывать составы преступлений, предусмотренных §§ 202a, 202b, 303a, 303b. Кроме того, уголовному законодательству в сфере регламентации ответственности за компьютерные преступления свойственна краткость изложения объективной стороны состава преступления, иными словами способы совершения деяний детально не конкретизируются, а также отсутствует квалифицированная ответственность специальных субъектов преступлений. Компьютерные преступления в узком их смысле, предусмотренные УУ ФРГ, в большинстве могут быть совершены как с прямым, так и с косвенным умыслом.

Уголовное законодательство Французской Республики состоит из Конституции Франции 1958 г., международно-правовых актов, Уголовного кодекса Франции, других кодифицированных законов, некодифицированных уголовных законов и подзаконных актов. В УК Франции все преступные деяния сгруппированы по объекту посягательства в самостоятельные разделы с учетом ценности того или иного охраняемого блага. Отличительной чертой уголовного законодательства Франции также является регламентация ответственности юридических лиц (ст. 121-2). УК Франции предусматривает ответственность за совершение компьютерных преступлений в Книге II, устанавливающей ответственность за преступления и проступки против личности, Книге III, регламентирующей ответственность за имущественные преступления и проступки, и в Книге IV, содержащей положения об уголовной ответственности за преступления и проступки против нации, государства и общественного спокойствия[152].

[152] Уголовный кодекс Франции от 1 янв. 1992 г. // URL: https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719 (дата обращения: 17.07.17).

А. Г. Волеводз проводит деление компьютерных преступлений по УК Франции на преступления против безопасности компьютерной информации, преступления в информационном компьютерном пространстве и иные преступления в компьютерной сфере, которое, на наш взгляд, целесообразно дополнить с учетом внесенных в уголовное законодательство Франции изменений[153]. Таким образом, к компьютерным преступлениям по УК Франции можно отнести ряд составов преступлений, расположенных в различных его главах и разделах[154].

К преступлениям против безопасности компьютерной информации среди названных выше составов преступлений, расположенных в УК Франции, мы можем отнести только ст.ст. 323-1, 323-2, 323-3, 323-3-1, 323-4, 323-4-1, 323-5, 323-6, расположенные в Главе III «Посягательства на системы автоматизированной обработки данных». Таким образом, в УК Франции находят отражения большее количество способов совершения преступлений, что в некоторой степени отличает его от других кодексов зарубежных стран. Внимание привлекает уголовно-правовая охрана *государственных систем обработки персональных*

---

[153] См.: Волеводз А. Г. Уголовное законодательство об ответственности за компьютерные преступления: опыт разных стран / А. Г. Волеводз, Д. А. Волеводз // Правовые вопросы связи. 2004. № 1. С. 43-44.

[154] Это перехват, хищение, использование или предание огласке сообщений, передаваемых средствами дальней связи (ст. 226-15); осуществление или отдача указания об осуществлении автоматизированной обработки поименных данных без осуществления предусмотренных в законе формальностей (ст. 226-16); осуществление или отдача указания об осуществлении обработки этих данных без принятия всех мер предосторожностей, необходимых для того, чтобы обеспечить безопасность данных (ст. 226-17); сбор и обработка данных незаконным способом (ст. 226-18); ввод или хранение в памяти ЭВМ запрещенных законом данных (ст. 226-19); хранение определенных данных сверх установленного законом срока (ст. 226-20); использование данных с иной целью, чем это было предусмотрено (ст. 226-21); разглашение данных, могущее привести к указанным в законе последствиям (ст. 226-22); деяния, связанные и изготовлением и распространением по телекоммуникационным сетям детской порнографии (ст. 227-23); незаконный доступ к автоматизированной системе обработки данных или незаконное пребывание в ней (ст. 323-1); воспрепятствование работе или нарушение работы компьютерной системы (ст. 323-2); ввод обманным путем в систему информации, а также изменение или уничтожение содержащихся в автоматизированной системе данных (ст. 323-3); использование полученных сведений в служебной деятельности для совершения преступлений, предусмотренных ст.ст. 323-1 по 323-3 (323-3-1); особые формы соучастия в преступлениях, предусмотренных ст.ст. 323-1 и 323-1-1 (323-4 и 323-4-1); дополнительная ответственность физических лиц за совершение деяний, предусмотренных ст.ст. с 323-1 по 323-3-1 (323-5); ответственность корпораций за преступлений, предусмотренные ст.ст. с 323-1 по 323-3-1 (323-6); сбор или передача содержащейся в памяти ЭВМ или картотеке информации иностранному государству, уничтожение, хищение, изъятие или копирование данных, носящих характер секретов национальной обороны, содержащихся в памяти ЭВМ или в картотеках, а также ознакомление с этими данными посторонних лиц (ст. ст. 411-7, 411-8, 413-9, 413-10, 413-11); уничтожение, порча или хищение любого документа, техники, сооружения, оборудования, установки, аппарата, технического устройства или системы автоматизированной обработки данных или внесение в них изъянов (ст. 411-9); террористические акты, связанные с деяниями в области информатики (ст. 421-1).

данных, проявляющаяся в квалифицированных признаках рассматриваемых составов преступлений (ст.ст. 323-1, 323-2, 323-3 и 323-4-1).

Представляет определенный интерес способ описания объективной стороны изнасилования как вступление потерпевшим в контакт с исполнителем преступных действий благодаря использованию телекоммуникационных сетей в результате распространения сообщений, адресованных неопределенному кругу лиц[155]. Таким образом, французским законодателем введена уголовная ответственность за рассылку определенного вида спама.

Уголовное законодательство Франции содержится широкий перечень способов совершения преступления и детальная их регламентация, предусматривает высокие размеры штрафов, а также закрепляется ответственность юридических лиц. Если уголовное законодательство ФРГ предусматривает незначительные по сравнению размеры санкции в виде лишения свободы (2-3 года), то УК Франции этот вопрос решает практически идентично отечественному – предусматривается ответственность до 5-7 лет лишения свободы в зависимости от конкретного преступления. Кроме того, уголовными законами как Франции, так и ФРГ предусмотрены достаточно суровые штрафные санкции, которые могут исчисляться десятками тысяч евро. Существуют значительные различия в признаваемой степени общественной опасности компьютерных правонарушений и в способах описания признаков составов преступлений.

Таким образом, в УК зарубежных стран не прослеживается какого-то единого подхода к определению места уголовно-правовых норм, предусматривающих ответственность за рассматриваемые нами преступления. Структурно уголовные кодексы стран-участников СНГ разнятся не только по вопросу места нахождения главы (либо раздела) с такими составами преступлений, но и по выделениию их над уровнем объекта уголовно-правовой охраны как «общественная безопасность и общественный порядок»[156].

---

[155] См.: Уголовное право зарубежных стран. Общая и Особенная части : учебник для магистров / под ред. Н. Е. Крыловой. 4-е изд., перераб. и доп. М.: Юрайт, 2015. С. 299.

[156] Напр., УК РК, УК РБ, УК Франции и др.

Глава 3. Реализация общих положений теории квалификации преступлений применительно к преступлениям против безопасности компьютерной информации

§ 1. Особенности установления объекта преступления и предмета посягательства при квалификации содеянного

В науке к определению объекта преступления исторически сложилось несколько основных подходов. Еще в 1874 г. Н. С. Таганцев в качестве объекта преступления рассматривал юридическую норму *в ее реальном бытие*[157]. В 1924 г. А. А. Пионтковский давал определение объекту преступления как *общественным отношениям*, охраняемым всем аппаратом уголовно-правового принуждения[158]. Только с развитием Советской уголовно-правовой теории под ним стали обычно понимать общественные отношения, охраняемые уголовным законом, которым при совершении преступления причиняется вред либо создается угроза причинения вреда.

Следует признать, что определение объекта преступлений в качестве общественных отношений не является универсальным. Например, ведутся дискуссии по поводу того, в какой конкретно форме признавать объект преступлений против личности: в форме блага, ценности либо общественных отношений. Мы придерживаемся точки зрения, согласно которой в основе любого общественного отношения как раз и находятся тот или иной интерес либо конкретное благо[159]. Таким образом, блага, социальные ценности или интересы являются первоначально предпосылкой, по поводу которых возникают общественные отношения между различными субъектами.

---

[157] См.: Таганцев Н. С. Курс русского уголовного права: Часть общая. Книга 1: Учение о преступлении: [Выпуск 1] / [Сочинение] Н. С. Таганцева, профессора С.-Петербургского университета. СПб.: Типография М. Стасюлевича, 1874. С. 175.

[158] См.: Пионтковский А. А. Уголовное право РСФСР, часть Общая. М., 1924. С. 129-130.

[159] См.: Уголовное право России. Общая часть: Учебник / Под ред. Ф. Р. Сундурова, И. А. Тарханова. 2-е изд., перераб. и доп. М.: Статут, 2016. С. 212.

Под общественными отношениями понимаются обычно социальные *связи*, возникающие между людьми, обществом и государством. Причинить вред объекту возможно только путем воздействия на вещи материального мира либо разрыва социальных связей в общественных отношениях[160]. Считается, что структура общественных отношений включает в себя 1) носителей (субъектов) отношения; 2) предмета, по поводу которого существуют отношения; 3) общественно значимой деятельности (социальной связи) как содержания отношений[161]. Опираясь на указанную структуру, механизм причинения вреда общественным отношениям выглядит как посягательство на перечисленные элементы общественных отношений либо как разрыв связей между названными элементами.

Поэтому под *объектом преступления* следует понимать охраняемое уголовным законом общественное отношение, на которое направлено преступное посягательство и которому причиняется ущерб либо создается угроза его причинения[162].

Объекты преступлений принято разделять по вертикали и горизонтали. Мы придерживаемся четырехзвенного деления объекта по вертикали на общий, родовой, видовой (который также именуют в качестве группового или специального)[163] и непосредственный.

Общий объект уголовно-правовой охраны находит свое отражение в ч. 1 ст. 2 УК РФ. Д. А. Калмыков предлагает его дополнить специальным указанием на охрану информационной безопасности[164]. Это предложение весьма убедительно. Указание информационной безопасности наряду с другими основными объектами

---

[160] См.: Корнеева А. В. Теория и квалификация преступлений: учебное пособие для магистрантов. М.: Проспект, 2015. С. 17.

[161] См.: Дроздов А. В. Человек и общественные отношения. Л.: Изд-во ЛГУ, 1966. С. 23-30.

[162] См.: Уголовное право Российской Федерации. Общая часть: Учебник / Под ред. Л. В. Иногамовой-Хегай. М.: НИЦ ИНФРА-М, 2013. С. 48; Уголовное право Российской Федерации. Общая и Особенная части: Учебник / Под ред. А. И. Чучаева. М.: Контракт, 2016. С. 60; Уголовное право России. Общая часть: Учебник / Под ред. Ф. Р. Сундурова, И. А. Тарханова. 2-е изд., перераб. и доп. М.: Статут, 2016. С. 210.

[163] См.: Семернева Н. К. Указ. соч. С. 36.

[164] См.: Калмыков Д. А. Информационная безопасность: Понятие, место в системе уголовного законодательства РФ, проблемы правовой охраны : дис. … канд. юрид. наук. Казань, 2005. С. 38-39.

представляется актуальным, ибо служит предпосылкой ее выделения в качестве самостоятельного *родового* объекта уголовно-правовой охраны.

Родовой объект преступления представляет собой *совокупность однородных* общественных отношений, охраняемых единым комплексом уголовно-правовых норм. Под родовым объектом иногда понимается определенная *сфера* общественных отношений, которая включает в себя социальные ценности, блага и интересы. Родовой объект лежит в основе деления УК РФ на разделы, одним из которых является «Общественная безопасность и общественный порядок» (раздел IX УК РФ), содержащий в себе вид (группу) преступлений против безопасности компьютерной информации (гл. 28 УК РФ).

Законодатель, расположив главу 28 в разделе IX УК РФ, фактически признал, что родовым объектом изучаемых нами в настоящем исследовании преступлений следует рассматривать общественную безопасность и общественный порядок. Такого мнения (с некоторой конкретизацией) придерживаются А. В. Наумов, Т. М. Лопатина, В. Г. Степанов-Егиянц, А. И. Коробеев, А. С. Червоткин, Д. М. Молчанов и другие ученые[165].

На наш взгляд, если на период принятия УК РФ в 1996 г. такой вывод был достаточно обоснован, то сейчас такое положение не в полной мере отражает сущность изучаемого нами явления. Так, в одном разделе каждая из глав должна образовывать единое целое. Однако группа рассматриваемых нами преступлений (гл. 28 УК РФ) качественно выделяется среди других преступлений против общественной безопасности и общественного порядка. Существующее законодательное положение не учитывает активное проникновение информационных отношений во все сферы общественных отношений. Именно поэтому вышеуказанный подход к определению родового объекта преступлений

---

[165] См.: Наумов А. В. Указ. соч. С. 565; Лопатина Т. М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности : дис. … д-ра юрид. наук. М., 2006. С. 193; Дворецкий М. Ю. Указ. соч. С. 37; Смирнова Т. Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации : автореф. … канд. юрид. наук. М., 1998. С. 12; Степанов-Егиянц В. Г. Указ. соч. С. 127, 129; Воробьев В. В. Указ. соч. С. 55; Суслопаров А. В. Указ. соч. С. 124; Уголовное право Российской Федерации. Общая и Особенная части: Учебник / Под ред. А. И. Чучаева. М.: Контракт, 2016. С. 565; Уголовное право РФ. Особенная часть: Учебник / Л. В. Иногамова-Хегай и др.; Под ред. Л. В. Иногамовой-Хегай. М.: НИЦ ИНФРА-М, 2013. С. 163; Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. В. М. Лебедев. 14-е изд., перераб. и доп. М.: Юрайт, 2014. С. 803; Молчанов Д. М. Указ. соч. С. 550.

против безопасности компьютерной информации представляется уязвимым. В связи с этим полагаем необходимым пересмотреть такой подход к его оценке.

Нам близка точка зрения Д. А. Калмыкова, который в своей работе обосновал не только существование в действующем Уголовном кодексе объекта уголовно-правовой охраны в виде информационной безопасности, выявил его распространенность наряду с другими объектами уголовно-правовой охраны, но и пришел к выводу, что «преступное посягательство на *любой объект* уголовно – правовой охраны с точки зрения формальной логики (в самом общем смысле) означает, в том числе, и нарушение *информационного компонента* соответствующего объекта»[166]. Однако, как нам представляется, Д. А. Калмыков не рассматривает информационную безопасность ни в качестве родового объекта преступлений, ни в качестве группового объекта. Так, в качестве родового объекта преступлений, расположенных в гл. 28 УК РФ, исходя из теории о четырехзвенной структуры объекта преступления, которой придерживается автор, им признается совокупность всех охраняемых уголовным законом общественных отношений в области компьютерной информации, а группового – общественная безопасность и общественный порядок в области информационных отношений[167]. Другие ученые также признают наличие такого объекта уголовно-правовой охраны в виде информационной безопасности[168].

Представление об информационной безопасности как родовом объекте уголовно-правовой охраны, на наш взгляд, предполагает отнесение к ним преступлений, посягающих на *информационную сферу* Российской Федерации. Следовательно, в структуре УК РФ необходимо выделить раздел «Преступления против информационной безопасности». До этого времени в действующем уголовном законодательстве *преступления против информационной безопасности* характеризуются, как представляется, наличием дополнительного объекта уголовно-правовой охраны в виде *безопасности информационной сферы*.

---

[166] Калмыков Д. А. Указ. соч. С. 38.
[167] См.: Калмыков Д. А. Указ. соч. С. 109.
[168] См., напр.: Степанов-Егиянц В. Г. Указ. соч. С. 40; Мнацаканян А. В. Информационная безопасность в Российской Федерации: уголовно-правовые аспекты : дис. ... канд. юрид. наук. М., 2016. С. 83.

При этом *под информационной сферой* следует понимать общественные отношения, заключающие в себе совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети Интернет, сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений[169].

Информационная безопасность рассматривается как составляющая национальной безопасности Российской Федерации наряду с другими ее видами: государственной, общественной, экологической, экономической, транспортной, энергетической и безопасностью личности. Поэтому информационная безопасность России, охватывая все сферы человеческой жизнедеятельности, оказывает влияние на обороноспособность страны, государственную и общественную безопасность, экономический рост, развитие науки, технологии и образования, качество здравоохранения, в том числе и экологию. Это значит, что информационная безопасность проявляется себя не только как один из видов безопасности, но и как срез экономической, социальной, политической, военной, духовно-культурной и иных видов безопасности, т.е. тех видов безопасности, в которых информационные процессы занимают существенное место.

Под «безопасностью» традиционно понимается «положение, при котором не угрожает опасность кому-, чему-нибудь»[170]. Схожее понимание безопасности мы можем найти в толковом словаре В. И. Даля: «отсутствие опасности; сохранность, надежность»[171]. Такое определение дано через его отрицание, из которого следует, что безопасность – это отсутствие опасности. В законодательстве и литературе

---

[169] Доктрина информационной безопасности Российской Федерации : утв. указом Президента РФ от 5 дек. 2016 г. № 646 // Собр. законодательства Рос. Федерации. 2016. № 50, ст. 7074.
[170] Ожегов С. И. Словарь русского языка. 18-е изд. М.: Русский язык, 1986. С. 38.
[171] Даль В. И. Толковый словарь живого великорусского языка. В 4 тт. Т. 1: А-З. М.: АСТ, Астрель, 2007. С. 134.

прослеживаются два подхода к определению «безопасности»[172]. Одни авторы утверждают, что «безопасность» определяется через состояние защищенности объекта, а другие через состояние, при котором объекту не наносится вреда[173].

Под «информационной безопасностью» в одноименной Доктрине понимается «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства». Должную обеспеченность информационной безопасности представляется возможным рассматривать в качестве необходимого условия обеспечения национальной безопасности.

Одним из объектов обеспечения информационной безопасности является КИИ государства. В Федеральном законе «О безопасности критической информационной инфраструктуры Российской Федерации», вступающем в силу с 01.01.2018 г. (далее – ФЗ № 187-ФЗ), устанавливаются правовые и организационные основы, направленные на предупреждение компьютерных инцидентов и атак на объекты КИИ, безопасность КИИ раскрывается как «состояние защищенности критической информационной инфраструктуры,

---

[172] См.: О безопасности : Закон РФ от 5 марта 1992 г. № 2446-1 // Рос. газ. 1992. № 103. (утр. силу); О безопасности : федер. закон Рос. Федерации от 28 декабря 2010 г. № 390-ФЗ : принят Гос. Думой Федер. Собр. Рос. Федерации 7 дек. 2010 г. : одобр. Советом Федерации Федер. Собр. Рос. Федерации 15 дек. 2010 г. // Рос. газ. 2010. № 295; Рыбалкин Н. Н. Природа безопасности: дис. … д-ра филос. наук. М., 2003. С. 24; Нестеров С. В. Общественная безопасность как правовая категория // Аграрное и земельное право. 2012. №12 (96). С.103; п. 4 ст. 2 // Собрание законодательства РФ. 2011. № 1, ст. 48.

[173] См.: Актуальные проблемы информационного права : учебник / Под ред. И. Л. Бачило, М. А. Лапина. М.: Юстиция, 2016. С. 360; Мнацаканян А. В. Информационная безопасность в Российской Федерации: уголовно-правовые аспекты : дис. ... канд. юрид. наук. М., 2016. С. 29; Информационная безопасность и защита информации: Учебное пособие / Е. К. Баранова, А. В. Бабаш. М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. С. 7; Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]. М., 2010. С. 27; Стратегия национальной безопасности России: теоретико-методологические аспекты: Монография / С. Н. Бабурин, М. И. Дзлиев, А. Д. Урсул. М.: Магистр, 2012. С. 15; Защита информации: Учебное пособие / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. С. 13; Калмыков Д. А. Информационная безопасность: Понятие, место в системе уголовного законодательства РФ, проблемы правовой охраны : автореф. дис. … канд. юрид. наук. Казань, 2005. С. 4; Полякова Т.А. Правовое обеспечение информационной безопасности при построении информационного общества в России : автореф. дис. ... д-ра юрид. наук. М., 2008. 38 с.; Кубышкин А. В. Международно-правовые проблемы обеспечения информационной безопасности государства : автореф. дис. ... канд. юрид. наук. М., 2002. С. 30; Букалерова Л. А. Информационные преступления в сфере государственного и муниципального управления: законотворческие и правоприменительные проблемы : автореф. дис. … д-ра юрид. наук. М., 2007. С. 27; Башлы П. Н. Информационная безопасность и защита информации [Электронный ресурс]: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. М.: РИОР, 2013. С. 9.

обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак» [174].

В литературе наряду с понятием «информационная безопасность» используются термины «компьютерная безопасность», «защита информации» и «безопасность информации», которые необходимо различать.

Иногда понятия «компьютерная безопасность» и «информационная безопасность» отождествляются [175] . В таких случаях информационная безопасность перестает включать в себя полный объем рассматриваемых по существу вопросов. Однако процесс осуществления информационной безопасности заключается в обеспечении безопасности не только компьютерной инфраструктуры, но и в поддерживающей ее инфраструктуры, к которой в равной степени, помимо прочих, относятся также и жилищные, коммунальные системы, системы жизнеобеспечения, средства коммуникации и др.

С понятием «информационная безопасность» тесно связано понятие «защита информации». Если «информационная безопасность» рассматривается как состояние объекта, то «защита информации» – это определенный процесс [176]. «Защита информации» является составной частью обеспечения информационной безопасности. Сущность защиты информации, как справедливо отмечается в литературе, состоит в определении угроз информации и их комплексном предотвращении[177].

Из имеющихся в науке подходов к определению безопасности (компьютерной) информации, мы можем сделать вывод, что она представляет собой один из элементов, с помощью которого достигается общая –

---

[174] О безопасности критической информационной инфраструктуры Российской Федерации : федер. закон Рос. Федерации от 26 июля 2017 г. № 187-ФЗ : принят Гос. Думой Федер. Собр. Рос. Федерации 12 июля 2017 г. : одобр. Советом Федерации Федер. Собр. Рос. Федерации 19 июля 2017 г. // Офиц. Интернет-портал правовой информации. 2017. 26 июля. URL: http://www.pravo.gov.ru (вступает в силу с 1 января 2018 г.).

[175] См., напр.: Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. М.: Книжный мир, 2009.

[176] См.: Информационная безопасность: Учебное пособие / Т. Л. Партыка, И. И. Попов. 5-е изд., перераб. и доп. М.: НИЦ ИНФРА-М, 2014. С. 31.

[177] Основные положения информационной безопасности: Учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. М.: Форум, НИЦ ИНФРА-М, 2015. С. 7-8.

информационная безопасность, т.е. ее состояние[178]. Частная же цель (обеспечение безопасности информации) достигается во время определенного процесса – защиты информации.

В свою очередь, информационную безопасность следует понимать в праве, как состояние защищенности информации, технологий ее формирования и использования (информационной сферы), при котором объекту правовой охраны не наносится вреда либо отсутствует реальная угроза его нанесения.

Следует сказать, что в литературе и в законе в качестве средств (способов) реализации защиты информации в информационных системах выделяются как правовое, так и организационное и инженерно-техническое обеспечения[179]. Одним из способов обеспечения правовой охраны информационной безопасности является ее охрана различными отраслями права, в том числе гражданским, трудовым, административным и уголовным правом. Компьютерная безопасность, как отмечалось ранее, это состояние защищенности компьютерных и сетевых устройств от угроз различного характера.

Согласно вышеизложенному, мы можем определить *безопасность обращения компьютерной информации* как отсутствие причинение вреда или такой угрозы процессам распространения, хранения, производства либо ее использования.

Информационная безопасность сейчас не выделяется в качестве самостоятельного основного объекта преступного посягательства в структуре УК РФ. Поэтому информационные отношения в силу их динамичного характера обеспечиваются уголовно-правовой охраной наряду с ее основными объектами уголовно-правовой охраны.

Мы предлагаем ввести новый раздел УК IX[1] «Преступления против информационной безопасности», в который следует перенести существующую гл.

---

[178] См. подробнее: Основные положения информационной безопасности: Учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. М.: Форум, НИЦ ИНФРА-М, 2015. С. 7-8; См.: Степанов-Егиянц В. Г. Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации : уголовно-правовой аспект : дис. ... д-ра юрид. наук. М., 2015. С. 38.

[179] См.: А. П. Жук, Е. П. Жук, О.М. Лепешкин, А. И. Тимошкин. Указ. соч. С. 6; Актуальные проблемы информационного права : учебник / под ред. И. Л. Бачило, М. А. Лапина. М.: Юстиция, 2016. С. 374-375; ФЗ № 149-ФЗ.

28 УК РФ с соответствующими составами преступлений. При этом целесообразно будет в нем выделять и иные главы. К примеру, как предлагает И. А. Клепицкий, в нее может войти глава «Преступления против информационной безопасности в сфере использования документов», ввиду острой потребности в принятии обобщенной нормы о подлоге документов[180].

Видовой объект преступления – это наиболее близкие по своей природе общественные отношения, на которые посягают преступления, предусмотренные в одной и той же главе Особенной части УК РФ[181]. Сейчас видовой объект лежит в основе деления разделов на главы[182].

Основные подходы к определению видового объекта изучаемых преступлений можно разделить на две группы. Первая группа ученых видовым объектом составов рассматриваемых нами преступлений предлагает считать сферу компьютерной информации и определять его как безопасность компьютерной информации[183]. В качестве видового объекта преступления различные авторы также предлагают считать безопасность *в сфере информационных ресурсов*[184], *компьютерную безопасность*[185] или *информационную безопасность*[186]. Другая группа авторов видовой объект определяет преимущественно через соответствующие общественные отношения[187].

---

[180] См.: Качество уголовного закона: проблемы Особенной части: монография / отв. ред. А. И. Рарог. М.: Проспект, 2017. С. 298.

[181] См.: Уголовное право России. Общая часть: Учебник / Под ред. Ф. Р. Сундурова, И. А. Тарханова. 2-е изд., перераб. и доп. М.: Статут, 2016. С. 225.

[182] Некоторыми учеными предлагается его именовать «групповым», а также выделять среди него подгрупповые объекты. См., напр.: Галиакбаров Р. Р. Уголовное право. Общая часть. Краснодар: КубГАУ, 1999. С. 100; Семернева Н. К. Указ. соч.

[183] См.: Наумов А. В. Указ. соч. С. 565; Гаврилин Ю. В. Расследование неправомерного доступа к компьютерной информации: Учебное пособие / Под ред. Н. Г. Шурухнова. М.: Щит-М, 2001. С. 18; Калмыков Д. А. Указ. соч. С. 109; Абов А. И. Указ. соч. С. 21; Уголовное право. Особенная часть: Учебник. Издание второе исправленное и дополненное / Под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева. М.: Контракт : НИЦ ИНФРА-М, 2008. С. 550.

[184] См.: Дворецкий М. Ю. Указ. соч. С. 40.

[185] См.: Батурин Ю. М., Жодзишский А. М. Компьютерные правонарушения: криминализация, квалификация, раскрытие // Советское государство и право. 1990. № 12. С. 89.

[186] См.: Зинина У. В. Указ. соч. С. 37-38.

[187] См.: Литвинов Д. В. Исследование механизмов противодействия компьютерным преступлениям: организационно-правовые и криминалистические аспекты: монография / Д. В. Литвинов, С. В. Скрыль, А. В. Тямкин. Воронеж: Изд-во Воронеж. ин-та МВД России, 2009. С.47; Воробьев В. В. Указ. соч. С. 55; Уголовное право Российской Федерации. Общая и Особенная части: Учебник / Под ред. А. И. Чучаева. М.: Контракт, 2016. С. 565; Степанов-Егиянц В. Г. Указ. соч. С. 141; Уголовное право РФ. Особенная часть: Учебник /

Не все имеющиеся предложения отражают суть рассматриваемых преступлений. Некоторые из них расширяют объект уголовно-правовой охраны. Так, при таких посягательствах в качестве видового объекта могут выступать не любые «информационные отношения», а только протекающие в компьютерных системах. Поэтому *видовым объектом* рассматриваемых составов преступлений следует считать, соглашаясь с предложениями, имеющимися в литературе, *безопасность компьютерной информации*.

В литературе предлагаются разнообразные подходы касаемо нового наименования гл. 28 УК РФ[188]. Мы считаем, что наименование главы из структуры уголовного законодательства должно определяться через видовой объект уголовно-правовой охраны, а не через предмет преступления (как это следует из действующей редакции УК РФ). Более того, ст. 274^1 УК РФ значительно расширила круг непосредственных объектов уголовно-правовой охраны, включив в них не только компьютерную информацию, но и объекты КИИ РФ, признаки которых сейчас не ограничиваются видами компьютерной информации.

Таким образом, главу 28 УК РФ, на наш взгляд, следует именовать как «*Преступления против безопасности компьютерной информации*», а ее объектом уголовно-правовой охраны необходимо считать *состояние защищенности компьютерной информационной сферы, при котором ей не наносится вреда либо отсутствует реальная угроза его нанесения.*

Под *непосредственным объектом* преступления обычно понимается конкретное общественное отношение (социальное благо, ценность, интерес), на которое осуществляется непосредственное посягательство и которому причиняется ущерб. Он является частью видового объекта. В связи с тем, что каждый последующий вид объекта по вертикали заключается в содержание

Л. В. Иногамова-Хегай и др.; Под ред. Л. В. Иногамовой-Хегай. М.: НИЦ ИНФРА-М, 2013. С. 244; Суслопаров А. В. Указ. соч. С. 124.

[188] См., напр.: Крылов В. В. Информационные преступления – новый криминалистический объект // Российская юстиция. 1997. № 4. С. 23; Карпов В. С. Уголовная ответственность за преступления в сфере компьютерной информации : дис. ...канд. юрид. наук. Красноярск, 2002. С. 124; Степанов-Егиянц В. Г. Указ. соч. С.141; Сало И. А. Указ. соч. С. 55; Айсанов Р. М. Состав неправомерного доступа к компьютерной информации в российском, международном и зарубежном уголовном законодательстве : дис. ... канд. юрид. наук. М., 2006. С. 38.

предыдущего, непосредственный объект преступления может находить свое отражение в наименовании раздела, получать отражение непосредственно в конструкции состава преступления, либо не называться в диспозиции уголовно-правовой нормы, но подразумеваться и выявляться логико-юридическим путем.

Подходы к определению непосредственного объекта изучаемых преступлений в литературе можно классифицировать на две основные группы. К *первой* группе можно отнести идеи авторов, характеризующих его в обобщенном виде[189]. Другие ученые, определяя непосредственный объект рассматриваемой разновидности преступлений, раскрывают его более подробно[190]. Ко *второй* группе можно отнести авторов, которые конкретизируют непосредственный объект применительно к каждому из рассматриваемых составов преступлений[191]. Некоторые из них объективно утратили теоретическое значение ввиду внесенных законодателем изменений.

На наш взгляд, основным непосредственным объектом уголовно-правовой охраны в целях его установления при квалификации преступлений следует признавать в ст. 272 УК РФ – *безопасность* охраняемой законом компьютерной информации, обеспечиваемая ее правомерным доступом, ст. 273 УК РФ – *безопасность* компьютерной информации и средств защиты компьютерной информации, обеспечиваемая правомерным оборотом компьютерных программ и компьютерной информации, ст. 274 УК РФ – *безопасность* компьютерной информации, компьютерной техники, информационно-телекоммуникационных сетей и оконечного оборудования, обеспечиваемая соблюдением правил их

---

[189] См. подробнее: Дворецкий М. Ю. Указ. соч. С. 44; Уголовное право России. Особенная часть: Учебник / Отв. ред. Б. В. Здравомыслов. М.: Юристъ, 1996. С. 350; Калмыков Д. А. Указ. соч. С. 109.

[190] См.: Смирнова Т. Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации : автореф. ... канд. юрид. наук. М., 1998. С. 12; Букалерова Л. А. Уголовно-правовая охрана официального информационного оборота / Под ред. В. С. Комиссарова, Н. И. Пикурова. М.: Юрлитинформ, 2006. С. 303; Лопатина Т. М. Указ. соч. С. 197.

[191] См.: Российское уголовное право. Особенная часть / Под ред. В. Н. Кудрявцева, А. В. Наумова. М.: Юристъ, 1997. С. 348, 350; Уголовное право Российской Федерации. Общая и Особенная части: Учебник / Под ред. А. И. Чучаева. М.: Контракт, 2016. С. 568-569; Хисамова З. И. Уголовно-правовые меры противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий : дис. … канд. юрид. наук. Краснодар., 2016. С. 130-139; Уголовное право России. Особенная часть: Учебник / Под ред. Ф.Р. Сундурова, М.В. Талан. М.: Статут, 2012. С. 611, 621, 623; Воробьев В. В. Указ. соч. С. 55; Воробьев В. В. Преступления в сфере компьютерной информации: юридическая характеристика составов и квалификация : дис. … канд. юрид. наук. Нижний Новгород, 2000. С. 44.

эксплуатации, а также безопасность информационно-телекоммуникационных сетей, обеспечиваемая соблюдением правил доступа к ним.

Непосредственным объектом преступления, ответственность за которое предусмотрена ст. 274[1] УК РФ, судя по закону, вступающему в силу с 1 января 2018 г., по месту будущего расположения нормы (ст. 274[1] УК РФ) в главе 28 УК РФ должна являться безопасность критической компьютерной информации, однако законодателем в конструкции состава преступления объект сформулирован шире: в виде безопасности объектов критической информационной инфраструктуры.

Объекты преступления по горизонтали принято разделять на основной, дополнительный и факультативный. Такое деление объекта по горизонтали вполне обосновано при рассмотрении сложных по своей природе общественных отношений, которым соответствуют сложные, составные преступления. Основной и дополнительный непосредственные объекты принимаются во внимание при квалификации преступлений[192]. Такое деление в уголовном законе имеет место только при их охране от посягательств на два и более разнородных объекта. Такие посягательства в литературе получили наименование в качестве многообъектных преступлений.

В качестве примеров могут выступать некоторые составы преступлений, которые при определенных обстоятельствах могут образовывать совокупность преступлений со ст.ст. 272-274[1] УК РФ и именуются в литературе как компьютерные преступления («киберпреступления», «высокотехнологические» преступления, преступления с использованием средств компьютерной техники и т.д.)[193].

---

[192] См.: Корнеева А. В. Указ соч. С. 18.

[193] Напр., это нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138); неправомерное вмешательство в работу Государственной автоматизированной системы Российской Федерации «Выборы» (ч.3 ст. 141); нарушение авторских и смежных прав (ст. 146)[193]; мошенничество в сфере компьютерной информации (ст. 159[6])[193]; уничтожение или повреждение имущества по неосторожности (ст.168)[193]; незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183); неправомерный оборот средств платежей (ст. 187); незаконные изготовление и оборот порнографических материалов или предметов (ст. 242), изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (ст. 242[1]), использование несовершеннолетнего в целях изготовления порнографических материалов или предметов (ст. 242[2]); государственная измена (ст. 275), шпионаж (ст. 276),

Под дополнительным объектом преступления обычно понимается общественное отношение, которое охраняется уголовно-правовой нормой наряду с основным объектом преступления и которому причиняется ущерб. Следует заметить, что нередко ценность дополнительного объекта уголовно-правовой охраны превышает ценность основного. Дополнительный объект преступлений против безопасности компьютерной информации имеет важное значение для их квалификации с учетом совокупности и квалифицированных признаков. В качестве таких дополнительных объектов могут выступать отношения собственности (ч. 2 ст. 272 УК РФ), интересы службы (ч. 3 ст. 272 УК РФ), жизнь и здоровье (ч. 4 ст. 272 УК РФ) и другие объекты.

В качестве дополнительного объекта уголовно-правовой охраны в основных составах неправомерного воздействия на КИИ РФ (ч. 1-3 ст. 274^1 УК РФ) выступают основные непосредственные объекты неправомерного доступа к компьютерной информации (272), создания, использования и распространения ВКП (273) и нарушения правил эксплуатации хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (274).

Отличие *факультативного объекта* преступления от дополнительного проявляется в отсутствии указания на него в конструкции основного состава преступления. В качестве факультативного объекта преступления могут рассматриваться иные объекты, охраняемые другими разделами и главами Уголовного кодекса[194].

Предмет посягательства включается в структуру объекта преступления, и его установление нередко позволяет выявить сам объект преступления. Под *предметом преступления* обычно понимается то, по поводу чего или в связи с чем возникает и функционирует общественное отношение. Вместе с тем в теории

диверсия (ст. 281), разглашение государственной тайны (ст. 283), незаконное получение сведений, составляющих государственную тайну (ст. 283^1) и другие составы преступлений.

[194] Например, конституционные права и свободы в случае нарушения авторских и смежных прав с использованием вредоносного компьютерного программного обеспечения. При неправомерном доступе к компьютерной информации или распространении вредоносных компьютерных программ либо иной компьютерной информации из хулиганский побуждений, в качестве факультативного объекта будет выступать общественный порядок; при неправомерном доступе к государственным сетям – безопасность государства.

уголовного права в связи усложнением современных общественных отношений в сфере компьютерной информации имеется неоднозначное понимание предмета преступления. Традиционно под предметом преступления понимаются только вещи материального мира, на которые оказываются воздействия преступным деянием. Такое положение возникает также в связи с потребностью осмысления и придания правовой формы некоторым «нематериальным» явлениям, таким, как электроэнергия, компьютерная информация и ряда других. Среди них особую актуальность приобретает правовая регламентация оборота криптовалют. Пробельность в уголовно-правовом регулировании проявляются в том, что криптовалюты не могут признаваться предметом преступлений. Вместе с тем, оборот криптобирж за 2016 г. в мире увеличился с 48 до 415 млн. долл.[195], а криптовалюта получает свое применение в качестве эффективного финансового инструмента не только на рынке повседневных товаров услуг, но и на «черном» и «сером» рынках.

При поиске решения проблемы некоторыми авторами определение предмета преступления дополняется признаком интеллектуальной ценности[196], другими – указанием на явления объективной действительности, которые можно с известной степенью точности воспринимать, измерять, фиксировать и оценивать[197], третьими – в дополнение к традиционному пониманию предмета перечисляются возможные исключения, согласно которым могут иметь место «беспредметные» составы преступлений[198].

Н. К. Семернева под предметом преступления понимает любой элемент общественного отношения, воздействуя на который лицо причиняет вред объекту преступления (видоизменяет, разрушает его)[199]. Впервые такое понимание предмета преступления было предложено В. К. Глистиным[200]. Он подчеркивает,

---

[195] См.: Сидоренко Э. Л. Криптовалюта как новый юридический феномен // Общество и право. 2016. №3 (57). С. 193.
[196] См.: Уголовное право Российской Федерации. Общая и Особенная части: Учебник / Под ред. А. И. Чучаева. М.: Контракт, 2016. С. 68.
[197] См.: Калмыков Д. А. Указ. соч. С. 44, 48.
[198] См.: Дуюнов В.К., Хлебушкин А.Г. Квалификация преступлений: законодательство, теория, судебная практика: Монография / 3-е изд. М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. С. 46.
[199] См.: Семернева Н. К. Указ. соч. С. 46.
[200] См.: Глистин В. К. Проблема уголовно-правовой охраны общественных отношений (объект и квалификация преступлений). Л.: Изд-во ЛГУ, 1979. С. 43.

что «только в структуре конкретного отношения или группы сходных отношений предмет "проявляет" свою функцию и накладывает "отпечаток" на содержание отношений»[201]. Представляется, что схожее свойство информации (зависимость от сферы отношений, в которой она обращается) было выявлено при рассмотрении философского понимания информации. Информация определяется только через конкретное содержание отношений, в которых она рассматривается. Следовательно, в качестве *предмета преступления следует рассматривать элемент общественных отношений, по поводу которого они складываются, и, воздействуя на который причиняется вред объекту преступления*.

Понятие предмета преступлений против безопасности компьютерной информации в литературе носит дискуссионный характер. В литературе в качестве их предмета рассматривается информация[202]. Из чего следует, что любая информация, вне зависимости от средств обработки и формы представления, может являться предметом преступлений против безопасности компьютерной информации. Такая позиция относительно предмета преступления страдает избыточностью, поскольку следует указывать, что она должна являться *компьютерной*.

Некоторые авторы в качестве предмета преступлений против безопасности компьютерной информации называют только компьютерную информацию[203]. Такой подход не представляется всеобъемлющим. Поэтому другие авторы в качестве предмета преступлений наряду с компьютерной информацией называют и некоторые другие элементы отношений[204].

Общепринято утверждение, что предметом рассматриваемых преступлений является *компьютерная информация*. В прим. 1 к ст. 272 УК РФ имеется указание на следующие существенные признаки *компьютерной* информации, согласно которым она должна быть 1) представлена в форме электрических сигналов, 2) не

---

[201] Глистин В. К. Указ соч. С. 45.
[202] См.: Суслопаров А. В. Указ. соч. С. 124.
[203] См.: Добровольский Д. В. Актуальные проблемы борьбы с компьютерной преступностью (уголовно-правовые и криминологические проблемы) : дис. ... канд. юрид. наук. М., 2005. С. 50; Степанов-Егиянц В. Г. Указ. соч. С. 125.
[204] См. подробнее: Вехов В. Б. Указ. соч. С. 23; Уголовное право Российской Федерации. Общая и Особенная части: Учебник / Под ред. А. И. Чучаева. М.: Контракт, 2016. С. 565, 568; Уголовное право РФ. Особенная часть: Учебник / Л. В. Иногамова-Хегай и др.; Под ред. Л. В. Иногамовой-Хегай. М.: НИЦ ИНФРА-М, 2013. С. 244, 247.

зависеть от средств их хранения, обработки и передачи. Подробная характеристика указанных признаков дана в § 1 Главы 2 настоящего исследования. В законе перечислены и другие признаки компьютерной информации, имеющие существенное значение для квалификации преступлений, которые не были нами рассмотрены. Такими признаками являются «*охраняемость законом*» (ст. 272 УК РФ), «*охраняемость*» без указание на закон (ст. 274 УК РФ). В диспозиции ст. 273 отсутствует указания на «охраняемость компьютерной информации» (ст. 273 УК РФ), что исключает необходимость ее установления.

Правоприменительная практика исходит из того, что одни авторы считают, что любая информация в той или иной степени охраняется законом, а указание в законе на рассматриваемый признак является излишним[205]. Но другие приходят к мнению о необходимости исключения рассматриваемого признака из диспозиции ст. 272 УК РФ[206]. Однако есть позиция, согласно которой уголовно-наказуемым будет являться неправомерный доступ только к охраняемой законом компьютерной информации[207]. Для ответа на вопрос, какая компьютерная информация является «охраняемой законом», обратимся к законодательству. Федеральный закон № 149-ФЗ в зависимости от доступа к компьютерной информации разделяет ее на общедоступную информацию и на информацию, доступ к которой ограничен. К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. Поэтому получение доступа к общедоступной компьютерной информации не может считаться неправомерным. Общедоступные сведения утверждаются в специальном перечне[208]. К охраняемой законом компьютерной информации необходимо, в первую очередь, отнести все сведения конфиденциального

---

[205] См.: Айсанов Р. М. Указ. соч. С. 59.
[206] См.: Волеводз А. Г. Противодействие к компьютерным преступлениям: правовые основы международного сотрудничества / А. Г. Волеводз. М.: Юрлитинформ, 2002. С. 84.
[207] См.: Уголовное право. Особенная часть: Учебник. Издание второе исправленное и дополненное / Под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева. М.: Контракт : НИЦ ИНФРА-М, 2008. С. 553.
[208] См.: Перечень сведений конфиденциального характера : утв. указом Президента РФ от 6 марта 1997 г. № 188 // Рос. газ. 1997. № 51.

характера, содержащиеся в Перечне сведений конфиденциального характера[209]. В качестве охраняемой на практике признается также налоговая, банковская тайна, персональные данные пациентов, сведения, перечисленные в Федеральном законе «О связи» (далее – ФЗ № 126-ФЗ), и др.[210]

Анализ правоприменительной практики позволяет сделать вывод, что установление признака «охраняемости законом» является достаточно простым, не требующим изучения большого количества нормативных правовых актов, устанавливающих механизмы охраны компьютерной информации[211]. Вместе с тем при квалификации деяний по ст. 272 УК РФ правоприменитель в некоторых случаях упускает из внимания важность установления закрепленного в законе признака «охраняемости» компьютерной информации. Так, в приговоре Советского районного суда г. Казани указывается, что лицо осуществило неправомерный доступ к информационной системе организации, но не раскрывается, почему эта система является *охраняемой* законом компьютерной информации[212].

На наш взгляд, указание в уголовном законе на признак «охраняемости законом» компьютерной информации в диспозиции рассматриваемых преступлений является избыточным. Если законодатель таким признаком предполагал позволить правоприменителю при квалификации самому оценить степень общественной опасности посягательства и не допустить привлечения к

---

[209] Персональные данные, служебная тайна, сведения, связанные с профессиональной деятельностью; сведения, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее); коммерческая тайна; сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них; сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц.

[210] Приговор Ново-Савиновского районного суда г.Казани Республики Татарстан от 18.10.16 г. по делу № 1-449/16 // ГАС «Правосудие». URL: http://novo-savinsky.tat.sudrf.ru (дата обращения: 13.07.17); Приговор Автозаводского районного суда г.Самары Самарской области от 04.08.16 г. по делу № 1-844/2016 // ГАС «Правосудие». URL: http://avtozavodsky.sam.sudrf.ru/ (дата обращения: 17.07.17); Постановление Советского районного суда г.Казани Республики Татарстан от 11.07.16 г. по делу № 1-416/2016 // ГАС «Правосудие». URL: http://sovetsky.tat.sudrf.ru/ (дата обращения: 13.07.17).

[211] См., напр.: Приговор Арского районного суда Республики Татарстан от 27.03.13 г. по делу № 1-16/13 // ГАС «Правосудие». URL: http://arsky.tat.sudrf.ru/ (дата обращения: 13.07.17); Приговор Менделеевского районного суда Республики Татарстан от 15.10.12 по делу № 1-89/12 // ГАС «Правосудие». URL: http://mendeleevsky.tat.sudrf.ru/ (дата обращения: 13.07.17); Приговор Зеленодольского городского суда Республики Татарстан от 04.06.13 г. по делу № 1-218/13 // ГАС «Правосудие». URL: http://zelenodolsky.tat.sudrf.ru/ (дата обращения: 13.07.17).

[212] Постановление Советского районного суда города Казани Республики Татарстан от 11.07.16 г. № 1-416/2016 // ГАС «Правосудие». URL: http://sovetsky.tat.sudrf.ru/ (дата обращения: 13.07.17).

уголовной ответственности лиц, не оказавших воздействие на *охраняемую* законом информацию, то такая цель оказалась неочевидной ввиду сформулированного в ч. 4 ст. 16 ФЗ № 149-ФЗ принципа, согласно которому обладатель самостоятельно обеспечивает охрану такой информации. Поэтому установление признака «охраняемости законом» компьютерной информации не всегда способно реализовать те функции, которые на него возлагал законодатель при конструировании нормы в 1996 г. Поэтому правоприменителем по смыслу закона в качестве охраняемой законом информации может рассматриваться любая информация, находящаяся на чужом компьютере, если она защищена собственником. Такое положение в целом соответствует букве закона, но лишает содержательности этот признак состава преступления, утверждающийся в виде «охраняемости законом».

При внесении изменений в ст. 274 УК РФ Федеральным законом № 420-ФЗ, а также при введении в УК РФ ст. 274^1 УК РФ ФЗ № 194-ФЗ, прослеживается уже отказ законодателя от признака «охраняемости *законом*». Законодатель не стал конкретизировать его указанием на «охраняемость» компьютерной информации именно законом, что представляется весьма целесообразным. Поэтому соответствующие изменения необходимо внести и в диспозицию ч. 1 ст. 272 УК РФ.

В части 2 ст. 274^1 УК РФ компьютерная информация как предмет посягательства дополняется указанием на еще один дополнительный признак: содержанием ее в критической информационной инфраструктуре Российской Федерации. Таким образом, предмет рассматриваемого преступления характеризуется местом его расположения в компьютерной технике, компьютерной сети и т.д., относящейся именно к указанной инфраструктуре.

Понятие *«компьютерная программа»*, на наш взгляд, тождественна понятию программе для электронно-вычислительных машин (ЭВМ). При этом понятие «ЭВМ» объективно устарело и поэтому изменениями, внесенными в 2011

г. в ст. 273 УК РФ ФЗ № 420-ФЗ, было заменено термином «компьютерная программа». Дефиниция «программы для ЭВМ» дается в ст. 1271 ГК РФ[213].

В. Б. Вехов справедливо утверждает, что целью определенного результата функционирования компьютерной программы, указанной в ст. 273 УК, является ее *вредоносность* [214]. В литературе предлагаются различные варианты определения ВКП [215]. Ее определение также содержится в некоторых нормативно-правовых актах[216].

Понятие «*вредоносной* компьютерной программы или иной компьютерной информации подобного рода» можно вывести путем толкования диспозиций ч. 1 ст. 273 УК РФ или ч. 1 ст. 274[1] УК РФ. Если ранее ВКП или иная компьютерная информация подобного рода разделялась на виды только в криминалистической теории, то законодательно с 1 января 2018 г. вводится в действие их классификация на два вида [217]. Как нам представляется, первый ее законодательный вид, согласно ч. 1 ст. 273 УК РФ, должен быть предназначен для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. На этот же вид по всей вероятности указывается и в ч. 2 ст. 274[1] УК РФ. Однако такое указание в диспозиции ч. 2 ст. 274[1] УК РФ без конкретизирующих ссылок на ч. 1 ст. 274[1] УК РФ либо ч. 1 ст. 274 УК РФ может

---

[213] Компьютерная программа - это представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения *определенного результата* (курсив – автора), включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения.

[214] См.: Вехов В. Б. Вредоносные компьютерные программы как предмет и средство совершения преступления // Расследование преступлений: проблемы и пути их решения: сб. науч.-практ. тр. М., 2015. № 2. С. 43-46.

[215] См.: Смирнова Т. Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: дис. ... канд. юрид. наук. М., 1998. С. 18; Дворецкий М. Ю. Преступления в сфере компьютерной информации. Научно-практический комментарий к главе 28 Уголовного кодекса Российской Федерации / М. Ю. Дворецкий. Тамбов, 2005. С. 112; Шарков А. Е. Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации : дис. ... канд. юрид. наук. Ставрополь, 2004. С. 129; Маслакова Е. А. Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты : дис. ... канд. юрид. наук. М., 2008. С. 9; Красненкова Е. В. Обеспечение информационной безопасности в Российской Федерации уголовно-правовыми средствами : дис. ... канд. юрид. наук. М., 2006. С. 124; Воробьев В. В. Преступления в сфере компьютерной информации ... С. 58.

[216] Напр., см.: Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г., г. Минск; Правила оказания телематических услуг связи : утв. постановлением Правительства РФ от 10 сент. 2007 г. № 575; ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»

[217] См. подробнее: Вехов В. Б. Компьютерные преступления: Способы совершения и раскрытия / Под ред. акад. В. П. Смагоринского. М.: Право и Закон, 1996. С. 78-86.

повлечь трудности при квалификации преступлений правоприменителем. Второй вид должен быть предназначен для неправомерного воздействия на КИИ РФ, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации.

Таким образом, первый вид ВКП либо иной компьютерной информации подобного рода является более широким определением по сравнению со вторым ее видом, которая предназначается исключительно для воздействия на КИИ РФ и являющимся более узким определением. Иными словами, рассматриваемые виды соотносятся как целое (общее) с частью (частным).

Второй вид ВКП либо иной компьютерной информации подобного рода, как нами отмечалось, должен быть предназначен для *неправомерного воздействия на КИИ РФ*. Понятие «воздействие» является достаточно широким. Под ним понимается обычно действие, имеющее целью повлиять на кого-нибудь, что-нибудь[218]. Если в ч. 1 ст. 274^1 УК РФ под неправомерным воздействием понимается, в том числе уничтожение, блокирование, модификация, копирование информации, содержащейся в КИИ РФ, то в ч. 2 ст. 274^1 УК РФ ссылка на такие последствия отсутствует. Представляется, что из-за не вполне удачного структурного построения ч. 2 ст. 274^1 УК РФ под неправомерным воздействием следует понимать в том числе уничтожение, блокирование, модификацию, копирование такой компьютерной информации. Кроме перечисленных в ч. 1 ст. 274^1 УК РФ действий, *под неправомерным воздействием на КИИ РФ следует понимать представление или распространение компьютерной информации, содержащейся в КИИ РФ*.

Неправомерным воздействием на КИИ РФ является, например, компьютерная атака, под которой понимается целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для

[218] Толковый словарь русского языка под ред. Д. Н. Ушакова. М.: Гос. ин-т Сов. энцикл., 1935-1940. URL: http://dic.academic.ru/dic.nsf/ushakov/762126 (дата обращения: 17.07.17).

организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации[219].

Исходя из этого, под *ВКП либо иной компьютерной информацией подобного рода* следует понимать представленную в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств, в целях несанкционированного (обладателем компьютерной информации) уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации либо неправомерного воздействия на КИИ РФ.

В качестве ВКП на практике признаются различные компьютерные вирусы, трояны, сканеры, патчеры, клавиатурные шпионы, логические бомбы и т.д. Например, действия Д. Альметьевским городским судом РТ были квалифицированы по ст. 273 УК РФ в связи с тем, что при совершении преступления он использовал патчер – программный продукт 3D_V13_antiHASP_v1.0.exe – для нейтрализации средств защиты программного продукта «Компас-3D V13»[220]. По другому делу действия К. квалифицированы по ст. 273 УК РФ, в связи с его использованием сканера DUBrute – ВКП, предназначенной для нейтрализации средств защиты компьютерных систем[221]. В некоторых случаях использование в преступной деятельности ВКП остается без надлежащей уголовно-правовой оценки. Так, не было должным образом оценено действие Н., который неправомерно установил программу «клавиатурный шпион» – ActualSpy, с помощью которой он получил пароли доступа к незаконно скопированной им компьютерной информации[222].

В качестве *иной вредоносной компьютерной информации* могут выступать упрощенные командные либо программные сценарии, файлы с набором

---

[219] п. 4 ст. 2 ФЗ № 187-ФЗ.
[220] Приговор Альметьевского городского суда Республики Татарстан от 05.07.12 г. по делу № 1-342 // ГАС «Правосудие». URL: http://almetevsky.tat.sudrf.ru/ (дата обращения: 13.07.17).
[221] Приговор Советского районного суда г. Казани Республики Татарстан от 17.08.16 г. по делу № 1-416/2016 // ГАС «Правосудие». URL: http://sovetsky.tat.sudrf.ru/ (дата обращения: 13.07.17).
[222] Приговор Авиастроительного районного суда г.Казани Республики Татарстан от 17.04.12 г. по делу № 90/12 // ГАС «Правосудие». URL: https://novo-savinsky.tat.sudrf.ru (дата обращения: 13.07.17).

инструкций («скрипты»), эксплоиты. Примерами скриптов являются «phpshell.php», «adminer-3.7.1.php», эксплоитов: «Microsoft Internet Explorer - mshtml.dll Remote Code Execution (MS17-007) Exploit», «Metasploit RPC Console Command Execution Exploit» и др. Так, Кировским районным судом г. Казани по делу Д. установлено, что он, воспользовавшись уязвимостью в ограничении по загрузке изображений на Интернет сайте, загрузил два скрипта «phpshell.php» и «adminer-3.7.1.php», являющихся вредоносными. Однако, соответствующая уголовно-правовая оценка при квалификации по ч. 1 ст. 273 УК РФ в приговоре не отражена[223].

Согласно материалам другого уголовного дела, С. путем фишинга получал регистрационные данные к электронным почтовым ящикам пользователей, в т.ч. доступ к их лицевым счетам денежной системы «Деньги Маил.Ру». Согласно заключению эксперта, на компьютере С. была обнаружена вредоносная компьютерная информация (наборы скриптов на универсальном языке программирования «PHP»), позволяющая путем фишинга незаконно получать регистрационные данные пользователей[224]. Таким образом, в действиях С. усматриваются признаки состава преступления, ответственность за которое предусмотрена ч. 1 ст. 273 УК РФ. Однако следователем соответствующие процессуальные решения по этому вопросу не были приняты.

В статье 273 УК РФ указывается, что негативные последствия преступления могут наступить в том числе и в отношении *средств защиты информации*. Под средствами защиты информации понимаются «технические, программные, программно-технические средства, вещества и (или) материалы, предназначенные или используемые для защиты информации»[225]. В качестве средств защиты компьютерной информации правоприменителем признаются аутентификационные данные (логины и пароли) службы «Удаленный рабочий

---

[223] Приговор Кировского районного суда г.Казани Республики Татарстан от 26.01.15 г. по делу № 1-19/2015 // ГАС «Правосудие». URL: http://kirovsky.tat.sudrf.ru/ (дата обращения: 13.07.17).
[224] Материалы уголовного дела № 917417 МВД по РТ ГСУ СЧ // Архив Советского районного суда г. Казани Республики Татарстан.
[225] Защита информации. Основные термины и определения. ГОСТ Р 50922-2006, утв. Приказом Ростехрегулирования от 27.12.2006 г. № 373-ст. М., Стандартинформ, 2008. С. 17.

стол» (Microsoft Windows)[226], системы условного доступа Viaccess, используемой оператором спутникового телевидения ОАО «НТВ-ПЛЮС» для защиты телевизионных каналов от несанкционированного просмотра» и др. [227].

В ст. 274 УК РФ дается указание на такие предметы преступления, как средства хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационные сети и оконечное оборудование, понятия которых в уголовном законодательстве не даются.

Средствами хранения, обработки или передачи компьютерной информации по своей сути являются компьютерные устройства. Так, в прим. 2 к ст. 286 МУК СНГ компьютер предлагается именовать как «компьютерное устройство» и понимать под ним универсальное программно-управляемое устройство, предназначенное для хранения, обработки и передачи данных, следуя ряду команд, способное выполнять множественные математические и логические операции, а также выполнять другие задачи манипулирования над символами и другими формами информации и выдающее результаты в форме, воспринимаемой человеком или другим компьютерным устройством. Такое понятие, на наш взгляд, является более удачным в отличие от существующего в нынешней редакции УК РФ. Его закрепление нам видится приемлемым в ФЗ № 149-ФЗ.

Под *информационно-телекоммуникационной сетью (далее – ИТС)* согласно ст. 2 ФЗ № 149-ФЗ понимается «технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники». К ним можно отнести домашние, общественные локальные сети, локальные сети предприятий, сеть Интернет. В материалах изученных судебных дел правоприменителем сеть Интернет зачастую признается средством совершения преступления[228].

---

[226] Приговор Московского районного суда г.Казани Республики Татарстан от 05.09.16 г. по делу № 1-259/2016 // ГАС «Правосудие». URL: http://moskovsky.tat.sudrf.ru/ (дата обращения: 13.07.17).
[227] Приговор Комсомольского районного суда г.Тольятти Самарской области от 27.04.12 г. по делу № 1-227/2012 // ГАС «Правосудие». URL: http://komsomolsky.sam.sudrf.ru/ (дата обращения: 13.07.17).
[228] Приговор Советского районного суда Республики Татарстан от 17.08.16 г. по делу № 1-416/2016 // ГАС «Правосудие». URL: http://sovetsky.tat.sudrf.ru/ (дата обращения: 13.07.17).

Согласно статье 2 ФЗ № 126-ФЗ «О связи», *оконечное (пользовательское) оборудование* – это «технические средства для передачи и (или) приема сигналов электросвязи по линиям связи, подключенные к абонентским линиям и находящиеся в пользовании абонентов или предназначенные для таких целей».

КИИ РФ будет являться предметом преступления, ответственность за которое будет установлена ст. 274^1 УК РФ с 01.01.2018 г. Согласно ФЗ № 187-ФЗ под «критической информационной инфраструктурой государства» предлагается понимать «объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов». Там же под «объектами КИИ» предлагается понимать информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры. Таким образом, следует признать, что рассматриваемый предмет преступления в ч. 3 ст. 274^1 УК РФ в своей регламентации страдает тавтологией и конструкции диспозиции можно было сформулировать проще с учетом ее бланкетного характера.

Понятие «информационная система» дается в ФЗ № 149-ФЗ. Под *информационной системой* следует понимать «совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств». Различают государственные, муниципальные и иные информационные системы. Под *информационной системой в КИИ РФ* – понимается та же совокупность информации, но относящаяся только к КИИ РФ[229].

Под *автоматизированной системой управления* согласно ст. 2 ФЗ № 187-ФЗ будет пониматься комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами[230].

---

[229] п. 3 ст. 2 ФЗ № 149-ФЗ.
[230] п. 1 ст. 2 ФЗ № 187-ФЗ.

Субъектами критической информационной инфраструктуры согласно тому же закону признаются государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Сеть электросвязи – это технологическая система, включающая в себя технические и программные средства, используемые для формирования, приема, обработки, хранения, передачи, доставки сообщений электросвязи, а также иные технические и программные средства, используемые при оказании услуг связи или обеспечении функционирования сетей связи, включая технические системы и устройства с измерительными функциями и линии передачи, физические цепи и линейно-кабельные сооружения связи, предназначенные для электросвязи, используемые для организации взаимодействия объектов КИИ РФ[231].

Таким образом, по основному непосредственному объекту уголовно-правовой охраны рассматриваемые составы преступлений возможно классифицировать на *два вида*. К первому виду относить составы преступлений, в которых в качестве непосредственного объекта уголовно-правовой охраны выступает безопасность компьютерной информации *общего* характера, обеспечиваемая различными способами уголовно-правовой охраны (ст.ст. 272-274 УК РФ). Ко второму виду – новый состав преступления, в котором основным непосредственным объектом уголовно-правовой охраны является безопасность объектов критической информационной инфраструктуры, обеспечиваемая

[231] п. 7, 24, 28 ФЗ № 126-ФЗ.

правомерным доступом к охраняемой компьютерной информации, содержащейся в КИИ РФ (ч. 2 ст. 274[1] УК РФ), правомерным оборотом компьютерных программ либо иной компьютерной информации (ч. 1 ст. 274[1] УК РФ), а также соблюдением правил эксплуатации и правил доступа к объектам КИИ РФ (ч. 3 ст. 274[1] УК РФ).

В качестве *предметом* рассматриваемых нами преступлений следует считать компьютерную информацию; ВКП или иную компьютерную информацию подобного рода; средства защиты компьютерной информации; средства хранения, обработки или передачи охраняемой компьютерной информации; информационные-телекоммуникационные сети; оконечное оборудование; объекты КИИ РФ; информационные системы; автоматизированные системы управления; сети электросвязи.

§ 2. Выявление признаков объективной стороны названных составов преступлений и деяний в процессе их квалификации

Объективная сторона преступления представляет собой проявление преступного поведения во внешнем, реальном мире. Это «внешний акт посягательства на охраняемые законом общественные отношения, протекающие в определенных условиях, месте и времени»[232], который представляет собой совокупность фактов, проявляющихся в деянии и его последствиях. Посредством извлечения юридически значимых признаков, он приводится в вид, пригодный для квалификации преступления.

Как отмечалось ранее, составы преступлений по описанию объективной стороны могут быть простыми и сложными. В конструкции составов преступлений против безопасности компьютерной информации деяния описываются различными способами: 1) как одно действие: «неправомерный доступ» (ст. 272); 2) как возможные альтернативные действия: «создание, распространение и (или) использование» (ч.1 ст.273 ст. 274[1]); 3) как деяние, выраженное в форме действия или бездействия: «нарушение правил» (ст. 274, ч. 3

[232] Семернева Н. К. Указ. соч. С. 50.

ст. 274[1]). Нарушение правил 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 неправомерной воздействия на КИИ РФ, или иных вредоносных компьютерных программ (ч. 2 ст. 274[1] УК РФ).

Перечисленные деяния являются особыми формами совершения преступлений, которые позволяют отграничивать один вид посягательства на компьютерную информацию от другого. Иными словами, при квалификации преступлений нормы, предусмотренные в ст.ст. 272-274 УК РФ, конкурируют между собой, отличаются непосредственно в деянии и схожи по иным признакам составов преступлений. Исключение составляет ст. 274[1] УК РФ, отличающаяся от других видов рассматриваемых преступлений, как нами отмечалось, основным непосредственным объектом посягательства.

Законодательство не содержит понятие *доступа* именно к компьютерной информации. В словаре русского языка под доступом понимается возможность проникновения куда-либо[233]. Согласно ГОСТу доступ к информации – это право, возможность, средства для поиска, извлечения или использования информации[234]. Под доступом к любой информации (а не только к компьютерной) в пп. 6 ст. 2 ФЗ № 149-ФЗ понимается *возможность получения* информации и ее *использования*. В литературе под «доступом к компьютерной информации» понимается *возможность воздействия* на компьютерную информацию[235].

Не следует уравнивать возможность получения лицом доступа к компьютерной информации с возможность ее уничтожения, блокирования,

---

[233] Словарь русского языка под ред. Д. Н. Ушакова. М.: Гос. ин-т Сов. энцикл., 1935-1940. URL: http://dic.academic.ru/dic.nsf/ushakov/794926 (дата обращения: 17.07.17).

[234] ГОСТ Р ИСО 15489-1-2007 «Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования».

[235] См.: Уголовное право России. Особенная часть: Учебник / Отв. ред. Б. В. Здравомыслов. М.: Юристъ, 1996. С. 353; Степанов-Егиянц В. Г. Указ. соч. С. 164.

модификации или копирования. Ибо возможность воздействия на компьютерную информацию в информационно-коммуникационной среде открывается только *при получении* лицом, совершающим преступление, определенных системных *прав* на чтение, запись информации или исполнение команд. Иными словами, при получении доступа к компьютерной информации лицо не всегда имеет возможность осуществить ее уничтожение, блокирование, модификацию или копирование. Действие по получению лицом права на чтение компьютерной информации и в случае наличия прямого умысла на копирование такой информации, следует квалифицировать как покушение на преступление. Таким образом, под *доступом* к компьютерной информации, по нашему мнению, следует понимать *получение лицом возможности воздействия* на компьютерную информацию в виде чтения, записи или исполнения в компьютерной системе команд.

Доступ к компьютерной информации должен осуществляться *неправомерно*. Из наличествующих определений неправомерности в литературе, сущность *неправомерного* доступа к охраняемой законом компьютерной информации, как нам представляется, заключается в том, что у лица отсутствуют законные основания для получения возможности воздействия на компьютерную информацию [236]. Так, Ново-Савиновским районным судом г. Казни верно квалифицированы действия А. в качестве неправомерного доступа к компьютерной информации, который, не имея разрешения на доступ к автоматизированному рабочему месту предприятия на момент совершения преступления, но обладая логином и паролем для доступа ввиду того, что ранее работал на этом предприятии и сам его устанавливал, считал, что компьютер и программное обеспечение принадлежат ему[237].

Наличие согласия лица, обладающего правомочиями собственника информации, не может являться признаком, определяющим неправомерность

---

[236] См.: Калмыков Д. А. Указ. соч. С. 113. Сизов А. В. Неправомерный доступ к компьютерной информации: практика правоприменения // Информационное право. 2009. № 1. С. 32-35.

[237] Приговор Ново-Савиновского районного суда г. Казани Республики Татарстан от 20.05.15 г. по делу № 1-14/15 // ГАС «Правосудие». URL: http://novo-savinsky.tat.sudrf.ru (дата обращения: 13.07.17).

доступа. Прежде всего необходимо установить *правомочие лица на получение информации*, в противном случае в диспозиции имело бы место указание на «несанкционированный» (неразрешенный) доступ вместо «неправомерного» доступа к информации. Понятие «неправомерность» является более узким по сравнению с понятием «несанкционированность». Представляется, что законодатель тоже различает эти определения, используя в диспозиции ст. 273 УК РФ дефиницию «несанкционированности», а в ст. 272 УК РФ и ст. 274^1 УК РФ – «неправомерности».

В качестве другого признака правомерности правоведами рассматривается защищенность информации[238]. Утверждается, что не может быть неправомерным доступ к информации, никак не защищенной, с чем мы также не можем согласиться. Часто компьютерная информация защищена соответствующими средствами защиты, но бывает, что никакие средства защиты компьютерной информации не применяются.

На практике признак неправомерного доступа к компьютерной информации не всегда находит правильное понимание при квалификации преступлений. Рассмотрим два различных варианта уяснения его признака. В качестве неправомерного доступа к охраняемой законом компьютерной информации стороной обвинения по делу квалифицированы действия Ф., неправомерно внесшей ложные сведения в базу данных ГИБДД в целях дальнейшей выдачи на основании этой информации водительских удостоверений[239]. Однако по делу было установлено, что Ф. имела законный доступ к работе с базой данных, что подтвердилось оформленным на ее имя соответствующим приказом и присвоенными ей аутентификационными данными, что послужило основанием для оправдания судом Ф. по ч. 2 ст. 272 УК РФ.

По другому делу Самарским областным судом указывается, что Х., имея логин и пароль для доступа к базе данных клиентов ОАО «Билайн», в силу

---

[238] См.: Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : дис. ... канд. юрид. наук. Владивосток, 2005. С.186; Сизов А. В. Указ. соч. С. 32-35.

[239] Приговор Приволжского районного суда г. Казани Республики Татарстан от 27.11.2013 г. по делу № 1-260/2013 // ГАС «Правосудие». URL: http://privolzhsky.tat.sudrf.ru/ (дата обращения: 13.07.17).

наделенных должностных полномочий по трудовому договору, в нарушение процедуры замены SIM-карт, утвержденной распоряжением руководителя, совершил доступ в модуль и внес изменения в список услуг и проведения абонентских операций с номерами клиентов, не имея соответствующих заявлений клиентов. Таким образом, правоприменитель квалифицировал действия Х. в качестве неправомерного доступа к компьютерной информации [240]. Поэтому необходимо уточнить, по отношению к чему относить признак «правомерности»? Непосредственно к доступу (к деянию), к уничтожению, блокированию, модификации, копированию (т.е. к последствиям), либо как к деянию, так и к последствиям? На наш взгляд, в первом приводимом нами примере признак неправомерности должен быть установлен из того, что Ф. в нарушение установленного регламента по выдаче водительских удостоверений вносила ложные сведения в базу данных ГИБДД. Исходя из противного толкования закона, остаются без надлежащей уголовно-правовой оценки деяния, представляющие явную общественную опасность.

В связи с этим нами предлагается в ч. 1 ст. 272 УК РФ «неправомерность» относить только к законодательно указанным последствиям, а не к самому доступу.

Деяние, предусмотренные в ч. 1 ст. 273, ч. 1 ст. 274^1 УК РФ, в виде *создания, распространения и (или) использования* компьютерных программ либо иной компьютерной информации перечисляются как альтернативные, поэтому выполнение какого-то одного из этих действий следует рассматривать в качестве оконченного преступления.

Формальный характер составов преступлений, а также размер санкции за такие деяния по сравнению с другими основными составами преступлений против безопасности компьютерной информации дает основание нам говорить, что законодатель признал указанные действия более общественно опасными. Основной состав создания, использования и распространения ВКП (ч. 1 ст. 273)

---

[240] Апелляционное постановление Самарского областного суда от 20.10.14 г. по делу № 22-4759/14 // ГАС «Правосудие». URL: http://oblsud.sam.sudrf.ru/ (дата обращения: 13.07.17).

по степени тяжести является преступлением средней тяжести, в отличие от двух других составов преступлений (ч. 1 ст. 272 и ч. 1 ст. 274), которые являются преступлениями небольшой степени тяжести.

Под *созданием* понимается нередко только *результат* такой деятельности[241]. Между тем, в науке уголовного права о моменте окончания создания вредоносной компьютерной программы существует две точки зрения. Согласно первой точке зрения, созданием вредоносной компьютерной программы признается любой *из этапов процесса* до ее окончательного «оформления», приведения в рабочее состояние[242]. Согласно второй, моментом окончания преступления признается рабочее, функционирующее состояние компьютерной программы, когда она может представлять непосредственную опасность наступления указанных в законе последствий[243]. Именно эта позиция разделяется автором настоящей работы. Поэтому нельзя соглашаться с позицией, что уголовная ответственность устанавливается за наличие исходных текстов вредоносных компьютерных программ на иных материальных носителях, отличных от машинных, в т.ч. бумажных[244].

Действительно, процесс создания ВКП либо иной компьютерной информации подобного рода чисто технически предполагает возможное прохождение некоторых этапов, стадий ее создания. Создание – это, прежде всего процесс, но не всегда результатом создания может являться работоспособная программа. Процесс создания компьютерной программы, по мнению ряда авторов, включает несколько этапов[245]. Из всех предлагаемых этапов первый

---

[241] Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. В. М. Лебедев. 14-е изд., перераб. и доп. М.: Юрайт, 2014. С. 807-808.

[242] См.: Дворецкий М. Ю. Указ. соч. С.109, 125; Волеводз А. Г. Указ. соч. С. 74-75; Добровольский Д. В. Указ. соч. С. 27; Маслакова Е. А. Указ. соч. С. 85; Геллер А. В. Указ. соч. С. 127; Зинина У. В. Указ. соч. С. 77; Саломатина Е. С. Распространение вредоносных программ для ЭВМ // Юридический вестник Ростовского Государственного экономического университета. 2007. № 2. С. 31-35.

[243] См.: Степанов-Егиянц В. Г. Указ. соч. С. 271; Ефремова М. А. Уголовная ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий: монография. М.: Юрлитинформ, 2015. С. 103.

[244] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России) // Документ опубликован не был. Доступ из справ.-правовой системы «Консультант Плюс». URL: http://www.consultant.ru (дата обращения: 27.07.17).

[245] Например, постановку задачи, определение среды существования и цели программы, выбор средств и языков реализации программы, написание алгоритма работы программы в виде исходного текста, перевод исходного

запуск рабочей версии вредоносной компьютерной программы, на наш взгляд, необходимо рассматривать как *использование* компьютерной программы, *а не как окончание процесса создания*. Ибо будучи неработоспособной компьютерная программа, если имеет место написание исходного кода на бумаге, не может представлять никакой опасности, а поэтому нельзя такую программу признать созданной[246]. В некоторых из своих постановлениях Пленум Верховного Суда РФ уже разъяснял понятие «создание», правда, применительно к другим видам преступлений, которые по общей логике соответствуют нашей позиции[247].

Таким образом, преступление, совершенное в виде *создания* ВКП либо иной компьютерной информации, следует считать *оконченным* тогда, когда такая программа либо компьютерная информация скомпилирована («собрана») в *рабочую версию* и готова к использованию. Иными словами, указанное преступление является оконченным с момента появления у лица фактической возможности использования вредоносных функций компьютерной программы или компьютерной информации.

Соответствующее правило квалификации может быть изложено следующим образом: любую стадию создания ВКП либо иной компьютерной информации подобного рода, исключающую возможность их использования по прямому назначению, по причинам, не зависящим от виновного лица, следует квалифицировать как *покушение* на преступление по ч. 3 ст. 30 и ч. 1 ст. 273 УК РФ.

текста программы на машинный язык (объектный код), компилирование программы, отладку программы, запуск и работу программы См. подробнее: Преступления в сфере компьютерной информации: квалификация и доказывание. Учебное пособие / Гаврилин Ю. В., Головин Ю. В., Кузнецов А. В., Толстухина Т. В. М.: Книжный мир, 2003. С. 35; Воробьев В. В. Указ. соч. С. 99; Дворецкий М. Ю. Преступления в сфере компьютерной информации (уголовно-правовое исследование) : дис ... канд. юрид. наук. Волгоград, 2001. С. 79.

[246] См.: Степанов-Егиянц В. Г. Там же.

[247] Например, в них указывалось, что «создание незаконного вооруженного формирования (часть 1 статьи 208 УК РФ) считается оконченным преступлением *с момента фактического образования* формирования (курсив наш – Р. Г.), то есть с момента объединения нескольких лиц в группу и приобретения хотя бы некоторыми из них оружия, боеприпасов, взрывных устройств, боевой техники»; «создание банды предполагает совершение любых действий, *результатом которых стало образование* (курсив наш – Р. Г.) организованной устойчивой вооруженной группы в целях нападения на граждан либо организации. Они могут выражаться в сговоре, приискании соучастников, финансировании, приобретении оружия и т.п.». См. постановление Пленума Верховного Суда РФ от 9 фев. 2012 г. № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» // Бюллетень Верховного Суда РФ. 2012. № 4; Постановление Пленума Верховного Суда РФ от 17 янв. 1997 г. № 1 «О практике применения судами законодательства об ответственности за бандитизм» // Бюллетень Верховного Суда РФ. 1997. № 3.

В судебной практике встречаются ошибки в квалификации преступлений, связанные с избыточным вменением лицу признака деяния в виде создания, который фактически отсутствовал. Так, в ходе рассмотрения уголовного дела судом из объема предъявленного обвинения было исключено указание на создание ВКП, поскольку фактически обвиняемым был только скопирован вредоносный компьютерный файл из сети Интернет[248].

Под *распространением* информации в законе понимаются действия, *направленные* на их *получение* неопределенным кругом лиц или ее *передачу* неопределенному кругу лиц[249]. Такое понимание можно применить и по отношению к распространению ВКП или иной компьютерной информации подобного рода. Однако словосочетание «передача неопределенному кругу лиц» не весьма удачно сформулировано и тяжело для восприятия. Представляется, что *передача* всегда конкретна и адресована какому-то лицу или кругу лиц.

Под таким распространением обычно понимается их передача как с помощью специальных носителей, сети, так и иным другим способом другому лицу[250]. Такое определение распространения было актуальным ранее, однако сейчас представляется довольно узким с учетом появления новых форм распространения ВКП или иной компьютерной информации подобного рода на практике. Поэтому сегодня недостаточно ограничиваться толкованием «распространения» только как передачи. При таком толковании «распространения» упускается из виду второй признак, имеющий существенное значение для понимания «распространения» – действий, направленных на предоставление возможности *получения* компьютерной информации другим лицом.

Передача ВКП либо иной компьютерной информации подобного рода возможна путем продажи, проката, сдачи внаем, предоставления взаймы. Иными словами, посредством совершения любых сделок. Названный способ

---

[248] Приговор Вахитовского районного суда г.Казани Республики Татарстан от 08.12.14 г. по делу № 1-450/2014 // // ГАС «Правосудие». URL: http://vahitovsky.tat.sudrf.ru/ (дата обращения: 13.07.17).
[249] п. 9 ст. 2 ФЗ № 149-ФЗ.
[250] См.: Уголовное право России. Особенная часть: Учебник / Под ред. Ф. Р. Сундурова, М. В. Талан. М.: Статут, 2012. С. 622.

распространения путем передачи является *активным способом их распространения*. Действия, направленные на предоставление возможности *получения* компьютерной информации другим лицом, могут выражаться в загрузке ВКП либо иной компьютерной информации подобного рода на файловой сервер и публикация ссылки на ее скачивания в сети Интернет, что позволяет неопределенному кругу лиц осуществить к ним доступ. Предлагаем такой способ именовать в качестве *пассивного распространения* ВКП или иной компьютерной информации подобного рода. Так, Магаданским городским судом по делу установлено, что Р. поместил в записанные на машинном носителе своего персонального компьютера папки вредоносную программу «KOMPAS-3D_V13_antiHASP_v1.0.exe» и с помощью программы-клиента «Greylink DC++, версия 0.58» предоставил абонентам сетевой инфраструктуры г. Магадана беспрепятственный удаленный доступ к данной вредоносной программе, осуществляя указанным способом в автоматическом режиме ее незаконное распространение[251].

Необходимым признаком «распространения» является получение или наличие возможности их получения *другим лицом*. Поэтому копирование или перенос ВКП либо иной компьютерной информации подобного рода с одного материального носителя на другой, принадлежащих обвиняемому, ошибочно квалифицировать в качестве распространения.

Важным признаком вменения в вину распространения в качестве оконченного деяния является также установление факта их *передачи* другому лицу и факта их размещения, *доступным* для копирования в зависимости от способа распространения.

ВКП может иметь свойство самораспространяться без участия виновного. В таком случае нельзя объективно вменять лицу действия, которые непосредственно им не совершались. Квалификацию в таких случаях следует проводить по признаку их «*использования*».

---

[251] Приговор Магаданского городского суда Магаданской области от 18.01.17 г. по делу № 1-58/2017 // ГАС «Правосудие». URL: http://magadansky.mag.sudrf.ru/ (дата обращения: 13.07.17).

Под *использованием* ВКП либо иной компьютерной информацией подобного рода в литературе понимается непосредственный выпуск ее в «свет», воспроизведение, распространение, копирование и иные действия по ее введению в хозяйственный оборот, в том числе в модифицированной форме[252]. К примеру, в качестве «использования» Советским районным судом г. Казани квалифицированы действия К., который совершил запуск программы, подбирающей аутентификационные данные (пары логин и пароль) к компьютерам в сети Интернет по заранее сформированному списку IP адресов[253].

Некоторыми исследователями предлагается введение уголовной ответственности за осуществление *иных, помимо указанных, действий* с ВКП либо иной компьютерной информацией подобного рода. В качестве примера называется их *хранение*[254]. Другие авторы отмечают, что из смысла ст. 273 УК РФ уже следует, что уголовно-наказуемым является деяние, как наличие исходных текстов вирусных программ, не рассматривая его в качестве самостоятельного[255]. В таком случае хранение программы ими отождествляется с ее использованием. Действия виде хранения и использовании вредоносных компьютерных программ и компьютерной информации такого рода в уголовном законодательстве должны различаться, как в конструкции других составов преступлений различается хранение и использование других предметов преступлений (ч. 2 ст. 146, 218, 220 УК РФ и др.).

Характеристика признака объективной стороны преступления в виде нарушения правил означает, что данная диспозиция является бланкетной. На деяние в виде *нарушения правил* содержатся указания в диспозициях ч. 1 ст. 274 и ч. 3 ст. 274^1 УК РФ. Объективная сторона этих составов преступлений сформулирована путем указания, прежде всего, на два вида нарушения правил: а) правил эксплуатации и б) правил доступа. Понятие «нарушение» должно

---

[252] См.: Вехов В. Б. Указ. соч. С. 43-46; Закон РФ № 3523-I от 23.09.1992 г. «О правовой охране программ для электронных вычислительных машин и баз данных» // (утр. силу)

[253] Постановление Советского районного суда г. Казани от 11.07.16 г. № 1-416/2016 // ГАС «Правосудие». URL: http://sovetsky.tat.sudrf.ru/ (дата обращения: 13.07.17).

[254] Степанов-Егиянц В. Г. Указ. соч. С. 277.

[255] См.: Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. В. М. Лебедев. 14-е изд., перераб. и доп. М.: Юрайт, 2014. С. 808.

означать, что лицо, обязанное в силу возложенных на него обязательств, вытекающих из иного нормативного акта, их не исполняет. Нарушать – значит действовать или бездействовать в противоречии с требованиями соответствующих норм.

На наш взгляд, нарушение *правил эксплуатации*, содержащихся в справочных инструкциях производителей средств хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационных сетей и оконечного оборудования, сами по себе не образуют состава рассматриваемого преступления. Правила, за нарушение которых установлена уголовная ответственность, могут содержаться только в нормативно-правовых актах и в локальных актах организаций. На лицо, являющееся субъектом данного преступления, должны быть возложены обязанности по соблюдению правил эксплуатации и доступа к соответствующей технике. Основными документами, регламентирующими рассматриваемые правила, являются ГОСТ Р МЭК 60950-2002 и СанПиН 2.2.2/2.4.1340-03[256]. Отсутствие обязанности лица по соблюдению указанных правил исключает уголовную ответственность лица[257].

В ч. 2 ст. 274 УК РФ указывается за нарушение: 1) правил эксплуатации а) средств хранения, обработки или передачи охраняемой компьютерной информации, б) информационно-телекоммуникационных сетей, в) оконечного оборудования; и 2) правил доступа а) к информационно-телекоммуникационным сетям. Часть 3 статьи 274^1 УК РФ устанавливает ответственность за нарушение: 1) правил эксплуатации а) средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ РФ; б) информационных систем, в) информационно-телекоммуникационных сетей, г) автоматизированных

---

[256] ГОСТ Р МЭК 60950-2002 «Безопасность оборудования информационных технологий» // утв. Постановлением Госстандарта России от 11.04.2002 г. № 148-ст. М.: Стандартинформ, 2005. URL: http://consultant.ru/ (дата обращения: 17.07.17); СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы» // утв. Постановлением Главного государственного санитарного врача РФ от 13 июня 2003 г. № 118. Зарегистрировано в Министерстве юстиции Российской Федерации 10.06.2013 г. за рег. № 4673.

[257] См.: Лопатина Т. М. Указ. соч. С. 214; Уголовное право. Особенная часть: Учебник. Издание второе исправленное и дополненное / Под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева. М.: Контракт : НИЦ ИНФРА-М, 2008. С. 561.

систем управления, д) сетей электросвязи, относящихся к КИИ РФ; и 2) правил доступа а) к информации, б) информационным системам, в) информационно-телекоммуникационным сетям, г) автоматизированным системам управления, д) сетям электросвязи. Такое законоположение позволяет говорить, что перечень нарушаемых правил эксплуатации и доступа в ст. 274 УК РФ, в отличие от указанных в ч. 3 ст. 274^1 УК РФ, представляется явно суженным.

К *факультативным признакам* объективной стороны преступления обычно относят преступные последствия, причинную связь между деянием и преступным последствием, место, время, обстановку, способ, орудия и средства совершения преступления[258]. Между тем, так называемые факультативные признаки могут быть признаны *обязательными* в составах преступлений, когда они указаны в качестве конструктивных или квалифицирующих (либо привилегированных) признаков. Не все перечисленные признаки в конструкциях рассматриваемых составов являются факультативными. В качестве конструктивного признака составов преступлений, предусмотренных ст.ст. 272, 274, 274^1 (ч. 2-3) 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 критической информационной инфраструктуре Российской Федерации (ч. 2 ст. 274^1, ч. 3 ст. 274^1)

Наступление одного из альтернативно перечисленных в ч.ч. 1 ст.ст. 272, 274, ч.ч. 2-3 ст. 274^1 УК РФ последствий будет образовывать *односоставное* преступление. Наступление нескольких последствий при одном деянии по общему правилу не будет образовывать совокупности преступлений, а должно квалифицироваться как единичное сложное преступление. Последствия,

---

[258] В литературе также встречается дискуссионная позиция об отнесении причинной связи и последствий к обязательным признакам объективной стороны преступления. Об этом см. подробнее: Куринов Б. А. Научные основы квалификации преступлений. М., 1984. С. 71; Уголовное право. Общая часть: Учебник для вузов / Отв. ред. И. Я. Козаченко. 5-е изд., перераб. и доп. М.: Норма, 2013. С. 186.

перечисленные в диспозициях основных составов ст.ст. 272, ч. 2-3 ст. 274[1] УК РФ, могут явиться причиной наступления иных, более значительных и тяжких последствий, наступление которых требует квалификации содеянного по совокупности преступлений. Правила квалификации в подобных случаях будут рассмотрены в следующей главе настоящей работы.

Иные последствия, не перечисленные в квалифицирующих и особо квалифицирующих частях составов преступлений, лежат за пределами *основного* состава преступления. В качестве таких последствий могут выступать, например, причинение материального ущерба *потерпевшему*. Так, по одному из уголовных дел в результате преступных действий К. информация, принадлежащая предприятию, была заблокирована и модифицирована, что причинило материальный ущерб на общую сумму 27 428 руб. 80 коп., выразившийся в проведении работ по восстановлению работоспособности[259].

Правильная квалификация преступлений с учетом последствий, указанных в составах преступлений против безопасности компьютерной информации, имеет важное значение. Так, по одному из рассмотренных нами дел, предварительными органами следствия в вину вменено копирование компьютерной информации. Проведенная экспертиза дала заключение о модификации компьютерной информации, которое явилось одним из оснований для исключения судом из обвинения 7 эпизодов по ч. 3 ст. 272 УК РФ[260].

Под *уничтожением* компьютерной информации понимается ее удаление из средств хранения компьютерной информации. Одной из особенностей такой информации является сложность ее полного уничтожения, что обусловливает наличие в уголовно-правовой науке различных точек зрений к пониманию ее уничтожения. Одна из распространенных позиций отличается тем, что только безвозвратное ее удаление является последствием, влекущим уголовную

---

[259] Приговор Советского районного суда г. Казани Республики Татарстан от 02.07.14 г. по делу № 1-437/2014 // ГАС «Правосудие». URL: http://sovetsky.tat.sudrf.ru/ (дата обращения: 13.07.17).

[260] Приговор Кировского районного суда г. Екатеринбурга Свердловской области от 28.12.16 г. по делу № 1-466/2016 г. // ГАС «Правосудие». URL: https://kirovsky.svd.sudrf.ru/ (дата обращения: 13.07.17).

ответственность[261]. Согласно другой точке зрения, при наличии возможности восстановления, необходимо такие действия квалифицировать как покушение на преступление [262]. Иные исследователи придерживаются мнения, что под уничтожением компьютерной информацией следует признавать удаление ее с памяти компьютерного устройства вне зависимости от возможности ее восстановления[263].

Бесспорным, на наш взгляд, является факт того, что уничтожение информации всегда влечет негативные последствия для ее обладателя. Зачастую уничтожение связано с причинением большого материального ущерба: простаивает технологический процесс организации, возникает необходимость в привлечении специалистов по восстановлению компьютерной информации, а степень восстановления информации также предстоит выяснить. Кроме того, умыслом деятеля зачастую может не охватываться наличие возможности восстановления компьютерных данных. Подобные обстоятельства могут быть учтены судом при назначении наказания виновному.

Поэтому нам близка позиция авторов, согласно которой под уничтожением компьютерной информации следует признавать ее удаление с средств хранения компьютерной информации вне зависимости от возможности ее восстановления.

На наш взгляд, применительно к компьютерной информации не совсем корректно использовать термин «уничтожение». Уничтожению могут быть подвергнуты вещи материального мира: имущество, документы, избирательные бюллетени, бухгалтерские или иные учетные документы, оружие, боеприпасы, взрывчатые вещества, взрывные устройства, наркотические средства, объекты культурного наследия и иные материальные предметы. В тоже время

---

[261] См.: Волеводз А. Г. Указ. соч. С. 67; Российское уголовное право. Особенная часть / Под ред. В. Н. Кудрявцева и А. В. Наумова. М.: Юристъ, 1997. С. 350; Сизов А. В. Квалификация нарушений правил эксплуатации ЭВМ, системы ЭВМ или их сети // Информационное право. 2007. № 4. С. 27-30; Омаров М. Д. Проблемы определения состава преступления за неправомерный доступ к информационным ресурсам информационных систем // Юридический вестник ДГУ. 2011. № 4. С. 56-58.

[262] См.: Быков В. М., Черкасов В. Н. Новый закон о преступлениях в сфере компьютерной информации: ст. 272 УК РФ// Российский судья. 2012. № 5. С. 14-19.

[263] См.: Ефремова М. А. Ответственность за неправомерный доступ к компьютерной информации по действующему законодательству // Вестник Казанского юридического института. 2012. № 8. С. 54-56; Кабанова А. Ж. Преступления в сфере компьютерной информации (уголовно-правовые и криминологические аспекты): автореф. дис. ... канд. юрид. наук. Ростов-на-Дону, 2004. С. 24; Степанов-Егиянц В. Г. Указ. соч. С. 176.

информацию, и не только компьютерную, представляется затруднительным уничтожить полностью. В том или ином виде или форме она, так или иначе, может сохраняться. Хотя на практике и встречаются случаи признания правоприменителем удаления компьютерной информации без возможности восстановления, она может быть восстановлена с помощью специального программного обеспечения [264] . Предлагаемый нами подход уже принят законодателем в качестве приемлемого в конструкции признака объективной стороны состава мошенничества в сфере компьютерной информации, в котором использован термин именно «удаление компьютерной информации».

Таким образом, *в составах преступлений против безопасности компьютерной информации представляется обоснованным замена термина «уничтожение» термином «удаление»*.

Изучение материалов уголовных дел показало, что при оценке признака «уничтожение» формальные ошибки в процессе квалификации преступлений против безопасности компьютерной информации имеют место ошибки формального характера. Так, Д. признана в совершенном с использованием незаконно полученных регистрационных данных (логина и пароля к принадлежащим потерпевшей электронным почтовым ящикам) неправомерном доступе через сеть Интернет к содержащейся в них охраняемой законом компьютерной информации и последующей ее модификации путем внесения изменений в ее содержание, а также изменении перечисленных регистрационных данных, вызвавшем блокирование доступа потерпевшей к указанной информации. Однако из описания преступного деяния в процессуальном акте не следовало, что действия осужденной повлекли уничтожение компьютерной информации: описательная и мотивировочная части приговора вступили в противоречие. При таких обстоятельствах вышестоящей судебной инстанцией

[264] См., напр.: Приговор Железнодорожного районного суда г. Самары от 29.12.15 г. по делу № 1-350/2015 // ГАС «Правосудие». URL: http://zheleznodorozhny.sam.sudrf.ru/ (дата обращения: 17.07.17).

признак «уничтожение компьютерной информации» был исключен из мотивировочной части приговора без изменения квалификации преступления[265].

Термин *блокирование компьютерной информации* раскрывается через категорию возможности использования компьютерной информации[266]. На наш взгляд, наиболее точное определение «блокирования» содержится в ГОСТе как «прекращение или затруднение доступа к информации лиц, имеющих на это право (законных пользователей)»[267].

Некоторые ведомственные органы при толковании «блокирования» обращают внимание, что важным его признаком является невозможность в течение некоторого времени осуществлять операции над компьютерной информацией[268]. Поэтому имеет место дискуссия по вопросу, в течение какого промежутка времени должно осуществляться блокирование компьютерной информации.

На наш взгляд, вопрос уголовно-правовой оценки такого деяния необходимо разрешать с учетом реальной общественной опасности такого деяния. При ее отсутствии следует признавать такие деяния малозначительными с учетом положения ч. 2 ст. 14 УК РФ.

Зачастую последствия в виде модификации и уничтожения компьютерной информации ведут к блокированию *другой* компьютерной информации. Так, некоторые суды в качестве блокирования признавали удаление компьютерной программы, воспрепятствовавшей доступ потерпевшего к участию в аукционе; удаление сайта организации, чем был заблокирован доступ посетителей к информации; изменение регистрационных данных для доступа к электронной почте, приведший к блокированию к ней доступа и др.[269] Под *модификацией*

---

[265] Апелляционное постановление Верховного суда Республики Татарстан от 25.10.13 г. по делу № 22-7993/2013 // ГАС «Правосудие». URL: http://vs.tat.sudrf.ru/ (дата обращения 17.07.17).

[266] См.: Степанов-Егиянц В. Г. Указ. соч. С. 176.

[267] ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» : утв. приказом Ростехрегулирования от 18 дек. 2008 г. № 532-ст. М.: Стандартинформ, 2009. С. 7. URL: http://нэб.рф (дата обращения 18.07.17).

[268] См.: Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации.

[269] Приговор Ново-Савиновского районного суда г. Казани Республики Татарстан от 20.05.15 г. по делу № 1-14/15 // ГАС «Правосудие». URL: http://novo-savinsky.tat.sudrf.ru (дата обращения: 13.07.17); Приговор Ново-Савиновского районного суда г. Казани Республики Татарстан от 18.04.16 г. по делу № 1-160/2016 // ГАС «Правосудие». URL:

компьютерной информации понимается любое изменение программного обеспечения, текстовых файлов, изображений, искажающих информацию по сравнению с ее первоначальным состоянием[270].

В качестве модификации правоприменителем признаются изменение логина и пароля, используемого для доступа к социальным сетям, внесение таких изменений в программу, которые делают ее неработоспособной или прекращают исполнение одной или нескольких ее функций, шифрование файлов базы 1С, исключающее возможность ее использования[271].

Правоприменитель в некоторых случаях под модификацией ошибочно понимает наличие любого изменения в компьютерной информации либо вменяет данный признак излишне в качестве ввода информации либо установки новой программы, что не приводит к модификации информации[272]. Поэтому *для правильного вменения указанного признака необходимо особое внимание уделять установлению причинно-следственной связи и содержанию и направленности умысла лица.*

Под *копированием компьютерной информации* понимается точное воспроизведение или запись компьютерной информации с одного носителя компьютерной информации на другой[273]. Под носителями компьютерной

---

http://novo-savinsky.tat.sudrf.ru (дата обращения: 13.07.17); Приговор Альметьевского городского суда Республики Татарстан от 15.03.13 г. по делу № 1-137/2013 // ГАС «Правосудие». URL: http://almetevsky.tat.sudrf.ru/ (дата обращения: 17.07.17); Приговор Железнодорожного районного суда г. Самары Самарской области от 29.12.15 г. по делу № 1-350/2015 // ГАС «Правосудие». URL: http://zheleznodorozhny.sam.sudrf.ru/ (дата обращения: 17.07.17).

[270] См.: Уголовное право. Особенная часть: Учебник. Издание второе исправленное и дополненное / Под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева. М.: Контракт, 2008. С. 556.

[271] Приговор Альметьевского городского суда Республики Татарстан от 12.11.12 г. по делу № 1-582 // ГАС «Правосудие». URL: http://almetevsky.tat.sudrf.ru/ (дата обращения: 17.07.17); Приговор Набережночелнинского городского суда Республики Татарстан от 24.10.13 г. по делу № 1-1196/13 // ГАС «Правосудие». URL: http://naberezhno-chelninsky.tat.sudrf.ru/ (дата обращения: 17.07.17); Постановление Советского районного суда г. Казани Республики Татарстан от 11.07.16 г. по делу № 1-416/2016 // ГАС «Правосудие». URL: http://sovetsky.tat.sudrf.ru/ (дата обращения: 13.07.17).

[272] См., напр.: Приговор Приволжского районного суда г. Казани Республики Татарстан от 27.11.13 г. по делу № 1-260/2013 // ГАС «Правосудие». URL: http://privolzhsky.tat.sudrf.ru/ (дата обращения: 13.07.17); Приговор Ново-Савиновского районного суда г. Казани Республики Татарстан от 20.05.15 г. по делу № 1-14/15 // ГАС «Правосудие». URL: http://novo-savinsky.tat.sudrf.ru (дата обращения: 13.07.17); Приговор Кировского районного суда г. Казани Республики Татарстан от 26.01.15 г. по делу № 1-19/15 // ГАС «Правосудие». URL: http://kirovsky.tat.sudrf.ru/ (дата обращения: 13.07.17).

[273] См.: Уголовное право России. Особенная часть: Учебник / Под ред. Ф. Р. Сундурова, М. В. Талан. М.: Статут, 2012. С. 616; См. напр.: Приговор Кировского районного суда г. Казани Республики Татарстан от 26.01.15 г. по делу № 1-19/2015 // ГАС «Правосудие». URL: http://kirovsky.tat.sudrf.ru/ (дата обращения: 13.07.17); Приговор Авиастроительного районного суда г. Казани Республики Татарстан от 17.04.12 г. по делу № 1-90/2012 // ГАС «Правосудие». URL: https://novo-savinsky.tat.sudrf.ru (дата обращения: 13.07.17).

информации понимаются материальные объекты, способные длительное время сохранять имеющуюся компьютерную информацию. Например, это магнитные диски (жесткие диски, гибкие диски и др.), оптические диски (CD, DVD и т.д.), переносные накопители данных (флэш-накопители) и др.

На наш взгляд, *не следует признавать общественно опасным копирование информации в пределах одной компьютерной техники*. Так, правоприменителем в качестве уничтожения, модификации и копирования квалифицировано создание зашифрованного архива, копирование папок и файлов в пределах одного магнитного жесткого диска и удаление системных файлов администратора с сервера[274].

Под *несанкционированным* уничтожением, блокированием, модификацией, копированием компьютерной информации (ст. 273 УК РФ) следует понимать действия, осуществляемые вопреки воле других лиц, которые не могут ими управляться, контролироваться, т.е. в отсутствии их разрешения и уведомления.

Поэтому для признания деяния преступным важно учитывать характер отношений правообладателя информации с лицом, осуществляющим посягательство на компьютерную информацию. Это позволяет отличать уголовно-наказуемое деяние от правомерных действий лиц. Такими лицами могут быть специалисты антивирусных компаний или специальных служб, разрабатывающие способы противодействия вредоносным компьютерным программам, выявляющие свойства и признаки таких компьютерных программ, или работники сервисных служб, обслуживающие компьютерную и периферийную техники. При ином толковании уголовного закона уголовной ответственности могли бы подлежать вышеуказанные лица.

В. Б. Вехов верно выделяет наиболее значимые признаки, которые позволяют определить характер *несанкционированности* действия компьютерной программы. Такая программа, по его мнению, не предполагает предварительного уведомления лица о характере действий и не запрашивает согласия у него на

---

[274] Приговор Ново-Савиновского районного суда г. Казани Республики Татарстан от 18.10.16 г. по делу № 1-449/16 // ГАС «Правосудие». URL: http://novo-savinsky.tat.sudrf.ru (дата обращения: 13.07.17).

реализацию своего назначения[275]. К примеру, в качестве несанкционированного признаются действия по модификации программного обеспечения из демонстрационной версии в версию, использование которой возможно лишь при наличии лицензионного соглашения с правообладателем[276].

Под *нейтрализацией средств защиты компьютерной информации* (ст. 273 УК РФ) следует понимать такое нарушение функционирования средств защиты компьютерной информации, при котором они прекращают выполнять свои функции. Некоторые исследователи считают нецелесообразным включение такого признака в конструкцию объективной стороны преступления по той причине, что он охватывается приготовительными действиями к неправомерному доступу к компьютерной информации[277]. Однако, исходя из представлений о стадиях совершения преступлений против безопасности компьютерной информации, каждое из деяний, описанных ст.ст. 273, 274, ч. 3 ст. 274^1 УК РФ, может выступать в качестве приготовления к неправомерному доступу к компьютерной информации. Поэтому такое положение не должно служить основанием для исключения даже какого-то одного предусмотренного законом признака. В судебной практике под нейтрализацией средств защиты, например, признается возможность использовать программу без аппаратного ключа доступа[278].

Проблемы при квалификации преступлений с учетом рассматриваемого признака также встречаются. Так, в качестве нейтрализации средств защиты компьютерной информации возможно было признать созданную ВКП, которая обладала правами администратора операционной системы, что давало возможность активировать функцию защиты от удаления данного вредоносного

---

[275] Вехов В. Б. Вредоносные компьютерные программы как предмет и средство совершения преступления // Расследование преступлений: проблемы и пути их решения: сб. науч.-практ. тр. М., 2015. № 2. С. 43-46.

[276] Приговор Альметьевского городского суда Республики Татарстан от 05.07.12 г. по делу № 1-324 // ГАС «Правосудие». URL: http://almetevsky.tat.sudrf.ru/ (дата обращения: 17.07.17).

[277] См.: Быков В. М., Черкасов В. Н. Новое об уголовной ответственности за создание, использование и распространение вредоносных компьютерных программ // Российский судья. 2012. № 7. С. 16-21; Степанов-Егиянц В. Г. Указ. соч. С. 281.

[278] Приговор Вязниковского городского суда Владимирской области от 11.10.11 г. по делу № 1-301/2011 // ГАС «Правосудие». URL: http://viaznikovsky.wld.sudrf.ru/ (дата обращения 18.07.17); Приговор Вахитовского районного суда г.Казани Республики Татарстан от 08.12.14 г. по делу № 1-450/2014 // ГАС «Правосудие». URL: http://vahitovsky.tat.sudrf.ru/ (дата обращения 18.07.17).

программного обеспечения[279]. Однако правоприменителем такая квалификация не отражена.

Преступление, предусмотренное ч. 1 ст. 274 УК РФ, является оконченным при наступлении последствия в *виде причинения крупного ущерба*. Согласно прим. 2 к ст. 272 УК РФ, крупным ущербом признается ущерб, сумма которого превышает один миллион руб. Как справедливо отметил Московский городской суд, по делу, квалифицированному по ч. 1 ст. 274 УК РФ, законодатель не устанавливает критериев причиненного ущерба, за исключением его размера, – суммы, превышающий один миллион руб., тем самым, отнеся его к категории оценочных понятий, зависящих и подлежащих определению в каждом отдельном конкретном случае как потерпевшим, так и уполномоченными на то участниками уголовного судопроизводства с учетом всех обстоятельств дела. Ущерб может быть причинен моральный, материальный, деловой репутации. К ущербу могут быть также отнесены вынужденные финансовые потери и затраты на восстановление рабочего состояния средств хранения, обработки или передачи охраняемой информации[280]. Например, Лефортовским районным судом г. Москвы установлено, что своими действиями А. причинил крупный ущерб ООО «Приват Трэйд» на общую сумму 1 155 600 руб.[281].

Причинение вреда КИИ РФ является последствие деяния, ответственность за которое предусмотрено ч. 2 ст. 274^1 УК РФ. Вред может наступать в результате уничтожения, блокирования, модификации, копирования, распространения

---

[279] Приговор Сызранского городского суда Самарской области от 16.11.15 г. по делу № 1-579/2015 г. // ГАС «Правосудие». URL: http://syzransky.sam.sudrf.ru/ (дата обращения 18.07.17).

[280] Апелляционное постановление Московского городского суда от 12.11.14 г. № 10-15427/2014 по делу № 1-277/14 // ГАС «Правосудие». URL: https://www.mos-gorsud.ru/ (дата обращения 18.07.17).

[281] Который выразился в вынужденных действиях, которые были проведены сотрудниками по восстановлению доступа к базе данных после смены всех паролей сотрудников, имеющих доступ к VPN-серверам, а также смены паролей в учетных записях серверов и сервисов ООО «Приват Трэйд» (общие затраты 388 000 руб.); проведению комплекса мероприятий, направленных на поиск лица, которое копировало информацию из базы данных (общие затраты 153 000 руб.); средний простой 115 сотрудников ООО «Приват Трэйд», имеющих доступ к VPN-серверам, из-за необходимости перенастройки VPN-серверов, составил 12 часов, то есть суммарно 920 часов на ожидание восстановления доступа к VPN-серверам, которые были оплачены ООО «Приват Трэйд» (общие затраты 414 000 руб.); покупке оборудования для сотрудников ООО «Приват Трэйд», взамен изъятого у А. по окончании служебной проверки (общие затраты 45 330 руб.); введению дополнительных средств учета лиц, осуществляющих доступ к базе данных ООО «Приват Трэйд», а также механизмов сохранения информации, направленных на недопущение копирования информации без согласования с руководством (общие затраты 155 270 руб.) См.: Постановление Лефортовского районного суда г. Москвы от 13.01.15 г. № 1-401/2014 по делу № 1-6/2015 // ГАС «Правосудие». URL: http://lefortovsky.msk.sudrf.ru/ (дата обращения 18.07.17).

компьютерной информации, содержащейся в КИИ РФ. Если неправомерный доступ к охраняемой компьютерной информации, содержащейся в КИИ РФ, *повлекший* уничтожения, блокирования, модификации, копирования, не приводит к причинению вреда КИИ РФ, то *деяние* следует квалифицировать по ч. 1 ст. 272 УК РФ.

При наличии деяния, за которым следуют общественно опасные последствия, для квалификации содеянного между ними необходимо установить наличие *причинно-следственной связи*. Под *причинной связью* понимается такое отношение между явлениями, при котором одно явление (причина) с определенной закономерностью способно породить другое явление (следствие)[282]. В теории уголовного права в качестве таких категорий рассматриваются деяние и его последствия. При определении детерминантного комплекса следует руководствоваться понятийным аппаратом философии и общефилософскими методами познаниями. Согласно теории необходимого и достаточного причинения последствия, они должны быть необходимыми, закономерными и достаточными результатами совершенного лицом деяния[283].

Понимание причинной связи в уголовном праве основывается на общем учении о причинении. Однако она имеет здесь свою интерпретацию. Так, причинно-связанными в уголовном праве считаются только рядом находящиеся (последовательно располагающиеся в причинно-следственном ряду) явления. Существуют некоторые правила установления причинной связи в процесс квалификации преступления: а) деяние (в качестве причины) по времени совершения должно быть раньше наступления вреда (рассматриваемого как следствие); б) между деянием (причины) и вредом (следствием) не должно быть промежуточных явлений (событий), способных оказать влияние на развитие

---

[282] См.: Уголовное право Российской Федерации. Общая часть: Учебник / Под ред. Л. В. Иногамовой-Хегай. М.: НИЦ ИНФРА-М, 2013. С. 75; Проблемы причины и причинной связи в институтах Общей и Особенной частей отечественного уголовного права: вопросы теории, оперативно-следственной и судебной практики / Злоченко Я. М., Козаченко И. Я., Курченко В.Н. С.-Пб., 2003. С. 24.

[283] См.: Проблемы причины и причинной связи в институтах Общей и Особенной частей отечественного уголовного права: вопросы теории, оперативно-следственной и судебной практики / Злоченко Я. М., Козаченко И. Я., Курченко В.Н. С.-Пб., 2003. С. 33.

причинно-следственного ряда; в) деяние (причина) по своим объективным свойствам должно быть способно причинить подобный вред (последствие).

В ч. 1 ст. 273 УК РФ указывается на определенные последствия, наступление которых охватывается познаниями субъекта, но их реальное наступление не определяет момент окончания преступления, ибо состав является формальным. Нельзя также говорить о факультативности таких последствий. Однако создание компьютерной программы, фактически не способной уничтожить компьютерную информацию, не должно влечь ответственности по ч. 1 ст. 273 УК РФ.

Таким образом, ответственность за преступления против безопасности компьютерной информации, составы которых сформулированы как материальные, может наступать только в том случае, если преступные последствия явились именно необходимым следствием, закономерно вызванным по воле лица, а не наступили в силу каких-либо иных причин.

Квалификация рассматриваемых преступлений с учетом требований правил установления причинно-следственной связи представляет определенную трудность, нередко влечет судебные или следственные ошибки. Особое внимание правоприменителю следует обращать на установление последствия в виде блокирования. Так, судом установлено, что Д. произвел неправомерный доступ к охраняемой законом компьютерной информации, повлекший копирование, модификацию и блокирование компьютерной информации при следующих обстоятельствах. Д. на сайте государственной организации обошел ограничения по загрузке изображений, загрузил два скрипта «phpshell.php» и «adminer-3.7.1.php», получил с помощью загруженного им скрипта доступ к базам с охраняемой в соответствии с Федеральным законом «О персональных данных» информацией, позволявший ему использовать функции чтения, модификации, создания и удаления данных. После чего скопировал вышеуказанные персональные данные и сохранил их. По сведениям потерпевшего, в результате «взлома» сайта на некоторое время была заблокирована его работа. Однако прямой причинной связи между неправомерным доступом к компьютерной

информации и блокированием сайта установлено не было, т.к. непосредственные действия обвиняемого к блокированию сайта не привели. Блокирование сайта было вызвано необходимостью его «отключения» для выявления и устранения уязвимости техническими специалистами, обслуживающими сайт[284].

Установление причинно-следственной связи между деянием лица и уничтожением (удалением) компьютерной информации является также необходимым условием правильной квалификации. Так, нельзя признавать уничтожением компьютерной информации переименование файла и автоматическое «вытеснение» старых версий файлов последними по времени[285].

Безосновательным следует признавать вменение следственными органами признака модификации, когда осуществляется изменение личной информации о состоянии счета вследствие использования логина и пароля потерпевшего в целях безвозмездного доступа к сети Интернет [286] . Правоприменителем квалифицировано содеянное по ч. 2 ст. 272 УК РФ.

Непосредственно такие действия не направлены на модификацию компьютерной информации и самостоятельной общественной опасности не несут, и поэтому не могут признаваться модификацией компьютерной информации. Совсем иначе выглядят ситуации, когда лицом искажается информация о состоянии лицевого счета, например, в целях увеличения баланса лицевого счета в большую сторону, создавая видимость, что им вносятся денежные средства, что позволяет ему безвозмездно пользоваться доступом к сети Интернет. Примером правильной квалификации является дело, по которому судом исключен из обвинения признак модификации компьютерной информации в связи с тем, что изменение данных по движению денежных средств по лицевому счету

---

[284] Приговор Кировского районного суда г.Казани Республики Татарстан от 26.01.15 г. по делу № 1-19/2015 // ГАС «Правосудие». URL: http://kirovsky.tat.sudrf.ru/ (дата обращения: 13.07.17).

[285] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации.

[286] Приговор Менделеевского районного суда Республики Татарстан от 15.10.12 г. по делу № 1-89/12 // ГАС «Правосудие». URL: http://mendeleevsky.tat.sudrf.ru/ (дата обращения: 18.07.17); Приговор Комсомольского районного суда г. Тольятти Самарской области от 27.10.10 г. по делу № 1-755/2010 // ГАС «Правосудие». URL: http://komsomolsky.sam.sudrf.ru/ (дата обращения: 18.07.17); Приговор Чистопольского городского суда Республики Татарстан от 04.05.12 г. по делу № 1-80/12 // ГАС «Правосудие». URL: http://chistopolsky.tat.sudrf.ru/ (дата обращения: 18.07.17).

потерпевших не является модификацией информации. Системой же были только зафиксированы факты доступа к лицевым счетам и факты перевода денежных средств[287].

Имеются проблемы при квалификации рассматриваемых преступлений и с учетом признака копирования компьютерной информации при установлении причинно-следственной связи. Так, В. В. Крылов справедливо полагает, что представляется ошибочным признавать в качестве последствия автоматическое копирование компьютерной информации, заключающееся в создании копии компьютерной информации без воли деятеля[288].

При конструировании рассматриваемых составов преступлений законодатель опирается нередко на такие признаки, как способ и средства совершения преступления. Под *способом совершения преступления* понимается внешняя форма, в которой выражаются преступные действия, а точнее приемы и методы, применяемые лицом, для совершения преступления[289]. В некоторых составах преступлений способ выступает в качестве факультативного признака преступления. Анализ ч. 1 ст. 272, ч. 1 ст. 273, ч. 1 ст. 274, ч.ч. 1-3 ст. 274[1] УК РФ убеждает в том, что *способы* совершения данных видов преступления значения для уголовно-правовой квалификации не имеют.

Под *средствами* и *орудиями совершения преступления* понимаются «методы действия (бездействия), одушевленные и неодушевленные компоненты, *используя* которые виновный воздействует на объект уголовно-правовой охраны»[290]. Четкого разделения орудий от средств совершения преступления не всегда приводится. Обычно отмечается, что применительно к группе насильственных и агрессивных преступлений точнее и удачнее использовать

---

[287] Приговор Промышленного районного суда г. Самары Самарской области от 04.10.16 г. по делу № 1-206/2016 // ГАС «Правосудие». URL: http://promyshleny.sam.sudrf.ru/ (дата обращения: 18.07.17).

[288] См.: Крылов В. В. Основы криминалистической теории расследования преступлений в сфере информации : дис. ... д-ра юрид. наук. М., 1998. С. 103; Волеводз А. Г. Указ. соч. С. 69; Озерский С. В. Указ. соч. С. 23; Степанов-Егиянц В. Г. Указ. соч. С. 193.

[289] См.: Уголовное право России. Общая часть: Учебник / Под ред. Ф. Р. Сундурова, И. А. Тарханова. 2-е изд., перераб. и доп. М.: Статут, 2016. С. 265; Уголовное право России. Части Общая и Особенная. 9-е издание. Учебник. Под ред. А. И. Рарога. М.: Проспект, 2017. С. 103.

[290] Уголовное право России. Общая часть: Учебник / Под ред. Ф. Р. Сундурова, И. А. Тарханова. 2-е изд., перераб. и доп. М.: Статут, 2016. С. 267.

термин «орудие преступления», а в отношении иных, ненасильственных деяний – «средства» совершения[291]. При таком понимании под ними следует понимать предметы, используемые в процессе насильственных посягательств непосредственно для воздействия на жизнь и здоровье человека. Тогда носители информации, средства преодоления защиты, периферийное оборудование, распространенные программные комплексы могут выступать в качестве средств совершения анализируемых преступлений, а не орудий. Эта точка зрения высказывается в литературе[292]. Анализ судебной практики квалификации таких преступлений позволяет нам сделать вывод, что они *всегда* совершаются с помощью средств компьютерной техники и программных средств.

Когда субъект осуществляет неправомерный доступ к охраняемой законом компьютерной информации, компьютерная информация является признаком *объекта*. Когда он использует компьютерную информацию *для* неправомерного доступа к охраняемой законом компьютерной информации, она становится средством посягательства. Компьютерная информация при определенных обстоятельствах может выступать в качестве средства совершения преступления, а не только в качестве предмета преступления[293]. Такая позиция нам представляется приемлемой, хотя в литературе высказываются и иные точки зрения[294].

Таким образом, нам представляется возможным сгруппировать изучаемые нами преступления на основании их отличия по характеру действий, их содержанию и регламентации по следующим *видам*, связанных 1) с неправомерным доступом к компьютерной информации (ст. 272, ч. 2 ст. 274[1] УК РФ); 2) с созданием, распространением и (или) использованием компьютерных

---

[291] См.: Уголовное право. Общая часть: Учебник. Издание второе переработанное и дополненное / Под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева. М.: Контракт : НИЦ ИНФРА-М, 2008. С. 156.

[292] См.: Степанов-Егиянц В. Г. Указ. соч. С. 209; Преступления в сфере компьютерной информации: квалификация и доказывание. Учебное пособие / Гаврилин Ю. В., Головин Ю. В., Кузнецов А. В., Толстухина Т. В. М.: Книжный мир, 2003. С. 116, 119.

[293] См. подробнее: Уголовное право России. Особенная часть: Учебник / Под ред. Ф. Р. Сундурова, М. В. Талан. М.: Статут, 2012. С. 609, 613; Вехов В. Б. Компьютерные преступления: Способы совершения и раскрытия. М.: Право и Закон, 1996. С. 23.

[294] См. подробнее: Зинина У. В. Указ. соч. С. 74; Козаев Н. Ш. Современные проблемы уголовного права, обусловленные научно-техническим прогрессом : дис. ... д-ра юрид. наук. Краснодар, 2016. С. 283.

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).

§ 3. Законодательное описание признаков субъективной стороны составов преступлений и проблемы ее установления в процессе квалификации содеянного

Субъективная сторона преступления характеризует «внутреннюю» сторону общественно опасного деяния, иными словами – это психическая деятельность лица, непосредственно связанная с совершением преступления. Являясь одним из элементов состава преступления, признаки субъективной стороны, как уже отмечалось, делятся на основные (вина) и факультативные (мотив, цель и эмоции), в совокупности образующие содержание субъективной стороны преступления.

В науке уголовного права устоялось понятие *вины*, определяемое как психическое отношение лица к совершенному деянию и наступившим общественно-опасным последствиям. Законодателем и в теории выделяются две формы вины (ст. 24 УК РФ): умысел и неосторожность, которые отличаются между собой особым сочетанием интеллектуальных и волевых моментов.

Интеллектуальный момент вины – это *осознание* лицом общественной опасности своего деяния; а также *предвидение* наступления общественно-опасных последствий (характерно для материальных составов преступлений). Волевой момент – *отношение* лица либо к самому деянию (в формальных составах преступлений), либо к наступившим последствиям моментам (в материальных составах преступлений).

В соответствии с положениями ст. 25 УК РФ умышленная форма вины выражается в двух ее видах: прямом (лицо осознавало общественную опасность своих действий (бездействия), предвидело возможность или неизбежность наступления общественно опасных последствий и желало их наступления) и косвенном (лицо осознавало общественную опасность своих действий

(бездействия), предвидело возможность наступления общественно опасных последствий, не желало, но сознательно допускало эти последствия либо относилось к ним безразлично).

По интеллектуальному моменту косвенный умысел отличается от прямого тем, что при последнем лицо предвидит неизбежность наступления общественно опасных последствий от своего деяния. При косвенном умысле лицо также их предвидит, но только реальную *возможность* (а не неизбежность) наступления преступных последствий.

В ст. 26 УК РФ указывается на наличие двух законодательных форм неосторожной вины: легкомыслия (лицо предвидит возможность наступления общественно опасных последствий своих действий (бездействия), но без достаточных к тому оснований самонадеянно рассчитывает на предотвращение этих последствий) и небрежности (лицо не предвидит возможность наступления общественно опасных последствий своих действий (бездействия), хотя при необходимой внимательности и предусмотрительности должно было и могло предвидеть эти последствия).

Неосторожность в виде легкомыслия следует отличать от косвенного умысла. Предвидение в косвенном умысле является реальной возможностью наступления последствий, а при легкомыслии – только абстрактной[295].

Конструктивным элементом субъективной стороны основных составов рассматриваемых нами преступлений является вина. Мотив и цели совершения преступления учитываются при конструировании квалифицированных составов. Нельзя согласиться с мнением, что эмоции являются признаком, образующим субъективную сторону преступлений против безопасности компьютерной информации[296]. Эмоции в качестве таковых выступают в ст.ст. 107 и 113 УК РФ.

Законодатель излагает субъективную сторону состава преступления разными способами, однако они всегда связаны с особенностями изложения объективной стороны его состава (характеристики) преступления. Иными словами, содержание

---

[295] См.: Семернева Н. К. Указ. соч. С. 99.
[296] См.: Дворецкий М. Ю. Указ. соч. С. 109, 131.

субъективной стороны состава преступления *выявляется* с учетом способа изложения объективной стороны характеристики в уголовном законе. Как известно, законодатель прямо может указать на форму вины, может указать на способ совершения деяния, позволяющий охарактеризовать форму вины, либо указать на цель или мотивы совершаемого деяния.

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.

По всем из изученных материалов уголовных дел правоприменителем доказывается и устанавливается наличие у лица специальных знаний в области компьютерной техники. Такие фактические данные дают основания полагать, что субъект действует осознанно и предвидит наступление тех или иных последствий при осуществлении определенных действий. Например, в приговоре Автозаводского районного суда г. Тольятти указывается, что К. осуществлял противоправные действия, обладая достаточными знаниями в области пользования компьютерной техникой[297].

Особенности определения формы вины и их видов не представляют возможности дать общего, универсального уголовно-правового анализа всех видов преступлений против безопасности компьютерной информации в их совокупности. В связи с этим каждый состав преступления следует, на наш взгляд, рассматривать в отдельности за исключением схожих между собой по объективной стороне составов преступлений.

По вопросу, какой вид умысла характерен *деянию, ответственность за которое предусмотрена основным составом неправомерного доступа к компьютерной информации (ч. 1 ст. 272 УК РФ),* в литературе прослеживается две позиции. Одни авторы полагают, что оно может совершаться только с прямым

[297] Приговор Автозаводского районного суда города Тольятти Самарской области от 13.04.16 г. по делу № 1-340/2016 // ГАС «Правосудие». URL: http://avtozavodsky.sam.sudrf.ru/ (дата обращения: 17.07.17).

умыслом[298], а другие обосновывают возможность его совершения с косвенным умыслом[299]. В силу схожести элементов составов преступлений, ответственность за которые предусмотрена ч. 1 ст. 272 и ч. 2 ст. 274[1] УК РФ, многие из рассматриваемых в них положений применимы друг к другу, однако по причине сложности их конструктивных характеристик они будут рассмотрены раздельно.

В связи с тем, что состав преступления, изложенный в ч. 1 ст. 272 УК РФ, является материальным, при анализе его субъективной стороны состава преступления и соотношения с объективной его стороной, к нему полностью применимы конструкции форм вины, предусмотренные ст.ст. 25, 26 УК РФ. В соответствии с описанием объективной стороны состава рассматриваемого преступления его субъективная составляющая строится на следующем сочетании интеллектуальных и волевых моментов. Составляющими интеллектуального и волевого элементов вины являются проблемы осознания, предвидения и волевого отношения к последствиям.

При характеристике данного состава предполагается, что интеллектуально субъект, во-первых, должен 1) *осознавать* фактические обстоятельства и общественную опасность (т.е. представляют определенную угрозу) *неправомерного* (вопреки закону или иным актам) доступа, т.е. существуют определенные правомерные способы доступа к такой информации; 2) *осознавать* то, что компьютерная информация, к которой осуществляется неправомерный доступ, *охраняется* законом. Во-вторых, деятелем должна *предвидеться* возможность или неизбежность наступления *последствий* в виде уничтожения, блокирования, модификации или копирования компьютерной информации, которая охраняется государством. Волевой элемент умысла указанного

[298] См.: Преступления в сфере компьютерной информации: квалификация и доказывание. Учебное пособие / Гаврилин Ю.В., Головин Ю. В., Кузнецов А. В., Толстухина Т. В. М.: Книжный мир, 2003. С. 26; Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. В. М. Лебедев. 14-е изд., перераб. и доп. М.: Юрайт, 2014. С. 805; Уголовное право. Особенная часть: Учебник. Издание второе исправленное и дополненное / Под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева. М.: Контракт, 2008. С. 552, 556; Дворецкий М. Ю. Указ. соч. С. 129.

[299] См.: Уголовное право. Особенная часть: Учебник. Издание второе исправленное и дополненное / Под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева. М.: Контракт, 2008. С. 552, 556; Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. В. М. Лебедев. 14-е изд., перераб. и доп. М.: Юрайт, 2014. С. 805; Комментарий к Уголовному кодексу Российской Федерации / Под ред. А. В. Наумова. М.: Юристъ, 1996. С. 665; Зинина У. В. Указ. соч. С. 68; Копырюлин А. Н. Указ. соч. С. 124-125; Наумов А. В. Российское уголовное право. Курс лекций. В двух томах. Т. 2. Особенная часть. М.: Юрид. лит., 2004. С. 568.

преступления характеризуется желанием субъекта наступления тех же последствий, что естественным образом допустимо. Таким образом, рассматриваемое преступление может совершатся с *прямым умыслом*.

В пользу возможности совершения этого вида преступления с косвенным умыслом ученые отмечают, что в последнем лицо деятель не всегда *желает* наступления вредных последствий, особенно при совершении преступлений из мотивов озорства или так называемого спортивного интереса, но сознательно их *допускает* [300]. Нежелание, но *допущение* последствий в виде уничтожения, блокирования, модификации, копирования компьютерной информации или безразличное отношение к ним может быть характерно в случаях, когда лицо ставит перед собой цель, например, визуального ознакомления с ней при том же спортивном интересе (доказать всем, кому-то, что он *может* получить неправомерно доступ к охраняемой законом компьютерной информации). Такие обстоятельства полностью обосновывают позицию возможности совершения неправомерного доступа к компьютерной информации (ч. 1 ст. 272 УК РФ) и с *косвенным умыслом*.

Так, приговором Автозаводского районного суда г. Тольятти К. осужден по ч. 1 ст. 272 УК РФ при следующих обстоятельствах. К., действуя в нарушение ФЗ № 149-ФЗ, неоднократно осуществил неправомерный доступ к охраняемой законом компьютерной информации (к программному обеспечению ЗАО «Банк Русский Стандарт» и банковской программе «Кредит», предназначенной для управления анкетами клиентов указанного Банка), используя незаконно полученные реквизиты сотрудницы «soldatkiname», внес сведения для последующего незаконного изготовления платежных банковских карт «Банк в кармане», без ведома последней, что повлекло модификацию компьютерной информации, то есть внесение изменений в программы, базы данных, текстовую информацию, находящуюся на материальном носителе указанного Банка[301]. В

---

[300] См.: Преступления в сфере компьютерной информации: квалификация и доказывание. Учебное пособие / Гаврилин Ю.В., Головин Ю. В., Кузнецов А. В., Толстухина Т. В. М.: Книжный мир, 2003. С. 26.

[301] Приговор Автозаводского районного суда г. Тольятти Самарской области от 13.04.16 г. по делу № 1-340/2016 // ГАС «Правосудие». URL: http://avtozavodsky.sam.sudrf.ru/ (дата обращения: 18.07.17).

связи с тем, что интерес К. был сконцентрирован на изготовлении платежных банковских карт «Банк в кармане», он мог безразлично относиться к модификации компьютерной информации в программном обеспечении банка, потому что неправомерный доступ не всегда может повлечь последствия в виде модификации компьютерной информации. Таким образом, нами не исключается оценка умысла внутренней стороны деятельности К. как совершенного с косвенным умыслом.

Возможность совершения преступления в виде неправомерного доступа к компьютерной информации по неосторожности рассматривается А. И. Коробеевым[302], С. А. Пашиным[303] и др. В частности, С. А. Пашин пишет, что «неосторожная форма вины может проявляться при оценке лицом правомерности своего доступа к компьютерной информации, а также неблагоприятных последствий доступа, предусмотренных диспозицией данной нормы уголовного закона»[304]. Другие авторы указывают, что по неосторожности рассматриваемый вид преступления не может совершаться ввиду отсутствия указания на неосторожную форму вины непосредственно в норме в соответствии со ст. 24 УК РФ[305].

При толковании ст. 24 УК РФ необходимо обратить внимание на разъяснения, данные в позициях высших судебных инстанций Российской Федерации. Согласно п. 4 постановления Пленума Верховного Суда РФ от 18.10.12 г. № 12, если в диспозиции статьи форма вины не конкретизирована, то соответствующее преступление может быть совершено умышленно или по неосторожности при условии, если об этом свидетельствуют содержание деяния, способы его совершения и иные признаки объективной стороны состава преступления[306]. Однако несколько иные разъяснения содержатся в п. 3.3

---

[302] См.: Уголовное право РФ. Особенная часть: Учебник / Л. В. Иногамова-Хегай и др.; Под ред. Л. В. Иногамовой-Хегай. М.: НИЦ ИНФРА-М, 2013. С. 247.

[303] См.: Комментарий к Уголовному кодексу Российской Федерации / Под ред. Ю. И. Скуратова и В. М. Лебедева. М.: Норма: ИНФРА-М, 1996. (автор главы - Пашин С. А.).

[304] Там же.

[305] См.: Преступления в сфере компьютерной информации: квалификация и доказывание. Учебное пособие / Гаврилин Ю.В., Головин Ю. В., Кузнецов А. В., Толстухина Т. В. М.: Книжный мир, 2003. С. 27.

[306] О применении судами законодательства об ответственности за нарушения в области охраны окружающей среды и природопользования : постановление Пленума Верховного Суда РФ от 18 окт. 2012 г. № 21 // Рос. газ. 2012. № 5924 (251).

постановления Конституционного Суда Российской Федерации от 31 марта 2011 г. № 3-П, согласно которому если в диспозиции статьи нет указания на совершение деяния по неосторожности, то предполагается, что оно может быть совершено только с умыслом[307].

Приведенные позиции содержат существенные противоречия, которые не позволяют с полной уверенностью определить, относится ли тот или иной состав преступления к умышленным или неосторожным деяниям.

Согласно ч. 2 ст. 24 УК РФ «деяние, совершенное *только* по неосторожности, признается преступлением лишь в случае, когда это специально *предусмотрено* (курсив наш – Р. Г.) соответствующей статьей Особенной части». Отсутствие непосредственного указания в диспозиции уголовно-правовой нормы слов «неосторожности» не может исключать возможность квалификации совершенного деяния как преступления, совершенного по неосторожности. Поэтому при принятии решения о том, может ли конкретное преступление совершаться с определенной формой вины или нет, необходимо в каждом составе преступления, исходить из анализа признаков *всей* уголовно-правовой нормы (диспозиции и санкции) и сопоставления с другими конкурирующими составами по *различным* их признаками.

В уголовно-правовой доктрине имеется мнение, что преступления, описываемые ч. 1 ст. 272 УК РФ и ч. 2 ст. 274^1 УК РФ, не могут быть совершены по неосторожности не потому, что отсутствует прямое указание на неосторожную форму вины, а в связи с тем, что на умышленный характер действий лица указывает наличие в норме слова «неправомерность» и виновный должен это осознавать[308]. На наличие умышленного характера действий лица в случае осознания им неправомерность своих действий указывает и М. Ю. Дворецкий. При этом он полагает, что факт *неправомерности* доступа лица к охраняемой законом

---

[307] Постановление по делу о проверке конституционности части третьей статьи 138 Уголовного кодекса Российской Федерации в связи с жалобами граждан С. В. Капорина, И. В. Коршуна и других : постановление Конституционного Суда Российской Федерации от 31 марта 2011 г. № 3-П // Рос. газ. 2011. №5454 (78).

[308] См.: Степанов-Егиянц В. Г. Указ. соч. С. 235.

компьютерной информации может подтверждаться обстоятельствами преодоления мер защиты компьютерной информации[309].

На наш взгляд, рассмотренная выше характеристика *предвидения* внешней стороны рассматриваемого преступления в некоторой степени характерна легкомыслию, но она должна *пониматься* субъектом. При легкомысленном совершении неправомерного доступа к компьютерной информации волевой момент субъекта характеризуется тем, что последствия, именованные в законе, *не наступят* с самонадеянным *расчетом* без достаточных на то оснований. Поэтому *этот* вид преступления против безопасности компьютерной информации представляется возможным совершить по легкомыслию.

Поскольку состав преступления, ответственность за которое предусмотрено ч. 2 ст. 274^1 УК РФ, является материальным, к нему также полностью применимы законодательные конструкции форм вины (ст.ст. 25, 26 УК РФ). Сфера *осознания* общественной опасности *деяния*, описанного в ч. 2 ст. 274^1 УК РФ, и *предвидения* последствий, образующих интеллектуальный момент, по содержанию достаточно объемны. Во-первых, деятель должен *осознавать* характер своего деяния: что доступ осуществляется *неправомерно*, т.е. понимать то, что им нарушаются определенные *правомерные* способы доступа к охраняемой законом компьютерной информации, содержащейся в КИИ РФ. Во-вторых, исполнитель преступления должен *осознавать*, что информация является *охраняемой законом*. В-третьих, *осознавать*, что компьютерная информация *содержится в КИИ РФ*. Иными словами, осознавать наличие всех признаков предмета преступления. В-четвертых, субъектом должен *заведомо*[310] *осознаваться* определенный *функционал* (их характеристика) двух видов средств совершения преступления: а) компьютерных программ либо иной компьютерной информации, *предназначенных* для неправомерного воздействия на КИИ; б) и иных ВКП (к которым также следует относить признак «*заведомости»* по причине ее указания в ч. 1 ст. 273 УК РФ, т.к.

---

[309] См.: Дворецкий М. Ю. Указ. соч. С. 115-117.

[310] Указание законодателем на заведомость, как справедливо указывает А. И. Рарог, особый технический прием (о котором упоминалось выше), означающий, что субъекту преступления заранее известно (т.е. заведомо) о наличии обстоятельств, имеющих существенное значение для квалификации преступления. См.: Рарог А. И. Проблемы квалификации преступлений по субъективным признакам: монография. М.: Проспект, 2016. С. 50.

именно она раскрывает признаки вредоносной компьютерной программы). В таком случае, при использовании лицом в процессе осуществления рассматриваемого преступления ВКП либо иной компьютерной информации подобного рода характерен только прямой умысел (ввиду заведомости).

В связи с тем, что элемент *предвидения* обращен к *последствиям*, лицо должно предвидеть, что его осознанные общественно опасные действия (указанные выше) приведут к возможности или неизбежности наступления *последствий* в виде вреда КИИ РФ (вторая часть интеллектуального момента умысла). Таким образом, указанное преступление при сочетании рассматриваемых признаков может быть совершено исполнителем преступления с прямым умыслом.

Волевой момент рассматриваемого преступления может характеризоваться *отношением* субъекта преступления к наступившим последствиям в виде вреда КИИ РФ не только как к желаемым (при прямом умысле), но и их допущением (при косвенном умысле). Поэтому, на наш взгляд, сфера интереса исполнителя рассматриваемого преступления может лежать вне пределов желания причинения законодательно предусмотренного вреда КИИ (например, при отсутствии желания причинения вреда такой информации при «спортивной» («игровой») мотивации деятельности). Однако им должны сознательно допускаться уголовно-наказуемые последствия, либо он должен относиться к ним безразлично. При прямом же умысле исполнителем преступления вся психологическая деятельность сосредоточена на осуществлении деяния *для того, чтобы* причинить *вред*, предусмотренный в диспозиции ч. 2 ст. 274^1 УК РФ.

Как было отмечено ранее, неосторожность определяется по отношению к последствиям. У субъекта при совершении рассматриваемого преступления, на наш взгляд, может иметь место *понимание* общественной опасности деятельной стороны рассматриваемого преступления, но иметься без достаточных оснований *расчет* (когда он полагается на себя, объективные факторы, определенную степень уверенности), что эти последствия не наступят, но только в том случае, когда указанное преступление совершается без использования любого из видов ВКП либо иной компьютерной информации подобного рода.

При небрежности субъект не предвидит наступления последствий, хотя должен был и мог их предвидеть. При осознании или даже понимании *неправомерности* доступа к охраняемой законом компьютерной информации не предвидеть какие-либо последствия, на наш взгляд, невозможно.

Таким образом, преступление, ответственность за которое предусмотрено ч. 2 ст. 274[1] УК РФ, с использованием ВКП либо иной компьютерной информации подобного рода (любого вида) возможно совершить только умышленно (характерен любой его вид). Неосторожностью в виде легкомыслия может характеризоваться только совершение этого преступления без использования указанных в нем средств преступления (ВКП либо иной информации подобного рода).

Распространенным мнением является, что преступление, предусмотренное основным составом *создания, использования и распространения ВКП или иной компьютерной информации (ч. 1 ст. 273 УК РФ),* может быть совершено только с прямым умыслом[311]. Между тем, по этому вопросу имеются иные взгляды ученых-правоведов[312].

Основные составы преступлений, ответственность за которые предусмотрена ч.ч. 1 ст. 273 и 274[1] УК РФ, являются формальными. Поэтому конструкции вины (ст.ст. 25, 26 УК) не применимы в полной мере (в части анализа предвидения и желания) при анализе субъективной стороны рассматриваемых преступлений ввиду отсутствия указания в них на последствия. Такое положение предопределяет возможность совершения их только умышленно, в отличие от квалифицированных *материальных* составов преступлений этого вида.

---

[311] См.: Уголовное право. Особенная часть: Учебник. Издание второе исправленное и дополненное / Под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева. М.: Контракт, 2008. 2008. С. 552, 559; Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. В. М. Лебедев. 14-е изд., перераб. и доп. М.: Юрайт, 2014. С. 808; Уголовное право РФ. Особенная часть: Учебник / Л. В. Иногамова-Хегай и др.; Под ред. Л. В. Иногамовой-Хегай. М.: НИЦ ИНФРА-М, 2013. С. 248; Уголовное право. Особенная часть: Учебник / Отв. ред. И. Я. Козаченко, Г. П. Новоселов. 5-е изд., изм. и доп. М.: Норма, 2013. С. 713; Дворецкий М. Ю. Указ. соч. С. 124; Наумов А. В. Российское уголовное право. Курс лекций. В двух томах. Т. 2. Особенная часть. М.: Юрид. лит., 2004. С. 570.

[312] См.: Преступления в сфере компьютерной информации: квалификация и доказывание. Учебное пособие / Гаврилин Ю.В., Головин Ю. В., Кузнецов А. В., Толстухина Т. В. М.: Книжный мир, 2003. С. 41; Уголовное право Российской Федерации. Общая и Особенная части: Учебник / Под ред. А. И. Чучаева. М.: Контракт, 2016. С. 567.

Осознание как интеллектуальный момент умысла характеризуется тем, что субъект преступления должен осознавать, во-первых, что осуществляет действия по созданию, использованию и («или» – при совершении преступления, ответственность за которое предусмотрено ч. 2 ст. 274^1 УК РФ) распространению. При совершении первого вида преступления (ч. 1 ст. 273 УК РФ) субъектом должны, во-вторых, осознаваться такие *свойства* предмета преступления, как их способность (т.е. *предназначенность*) 1) несанкционированно уничтожать, блокировать, модифицировать или копировать компьютерную информацию; 2) нейтрализовывать средства защиты компьютерной информации. При совершении второго вида преступления (ч. 1 ст. 274^1 УК РФ) способность компьютерных программ или компьютерной информации (предметов преступления) 1) неправомерно воздействовать на КИИ РФ, в том числе для (*путем*) а) уничтожения, блокирования, модификации, копировании информации, содержащейся в КИИ РФ; б) или *иным способом*, о котором свидетельствуют использованный союз «*в том числе*», позволяющий нам предполагать, что законодатель допускает *и иные способы* неправомерного воздействия на КИИ РФ, но также осознаваемые исполнителем преступления; 2) или нейтрализовывать средства защиты информации, содержащейся в КИИ РФ.

В уголовно-правовой литературе отмечается, что возможность совершения преступлений с косвенным умыслом не свойственна формальным составам преступления[313]. Указанный в законоположениях термин «*заведомость*» также характеризует именно умышленную форму вины в виде его *прямого* умысла. Такие знания лица исключают и неосторожную форму вины[314]. При этом требование «заведомости» обращено к *предмету* посягательства (компьютерной программе или компьютерной информации) и его *свойствам*.

Предвидения (как интеллектуального момента) и отношения (как волевого момента) субъекта преступления к последствиям невозможно *установить*,

---

[313] См.: Семернева Н. К. Указ. соч. С. 92; Рарог А. И. Проблемы квалификации преступлений по субъективным признакам: монография. М.: Проспект, 2016. С. 82.

[314] См.: Преступления в сфере компьютерной информации: квалификация и доказывание. Учебное пособие / Гаврилин Ю.В., Головин Ю. В., Кузнецов А. В., Толстухина Т. В. М.: Книжный мир, 2003. С. 42; Комментарий к Уголовному кодексу Российской Федерации / Под ред. А. В. Наумова. М.: Юристъ, 1996. С. 666.

поскольку последствия в составе законодателем не обозначены. Иными словами, даже при наличии в фактических данных (в совершенном преступлении) последствий, наступивших вследствие совершения деяния, то их мы не можем сопоставить (сравнить, установить тождество) с признаками объективной стороны состава преступления (последствиями), указания на которые отсутствуют в основных составах рассматриваемых преступлений.

Таким образом, созданию, использованию и распространению ВКП (ч. 1 ст. 273 УК РФ) и созданию, использованию и распространению ВКП, предназначенных для неправомерного воздействия на КИИ РФ (ч. 1 ст. 274^1 УК РФ), характерен только прямой умысел.

Правоприменитель при квалификации преступления, ответственность за которое предусмотрено ст. 273 УК РФ, ограничивается лишь указанием на то, что лицо действует умышленно, а также называет цели, которые, как представляется, позволяют ему делать такой вывод. Например, лицо совершило преступление умышленно, в целях проверки функциональных возможностей компьютерной программы [315], из корыстной заинтересованности [316]. Более того, в правоприменительной практике простое перечисление всех вмененных признаков субъективной стороны состава преступления является исключительным случаем. Из всех изученных нами материалов уголовных дел правоприменителем только в одном постановлении перечислены все ее признаки. Так, Самарским областным судом установлено, что доводы защиты об отсутствии в действиях Е. состава преступления, предусмотренного ч. 2 ст. 273 УК РФ, не основаны на материалах дела, опровергаются установленными фактическими обстоятельствами. Из показаний свидетелей следовало, что Е. пообещал предоставить компьютерный программный продукт. Согласно заключению эксперта и его показаний, на флеш-накопителе был установлен каталог, содержащий программу взлома защиты, которая позволяла пользоваться программами без ограничений. Таким образом, Е.,

---

[315] Приговор Советского районного суда города Казани Республики Татарстан от 11.03.16 г. № 1-731/2016 // ГАС «Правосудие». URL: http://sovetsky.tat.sudrf.ru/ (дата обращения: 13.07.17).

[316] Приговор Советского районного суда города Казани Республики Татарстан от 17.08.16 г. № 1-416/2016 // ГАС «Правосудие». URL: http://sovetsky.tat.sudrf.ru/ (дата обращения: 13.07.17).

используя вредоносную программу, осознавал общественную опасность своих действий, предвидел неизбежность наступления общественно опасных последствий в виде несанкционированного копирования информации и желал этого[317].

К вопросу о возможной форме вины, с которой совершается преступление, предусмотренное основным составом *нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ч. 1 ст. 274 УК РФ),* в литературе также неоднозначный подход. Первая группа авторов считает, что указанное преступление может образовывать состав преступления, совершенное как умышленно, так и по неосторожности[318]. Другие указывают, что оно может быть совершено только умышленно[319]. Третьи говорят только о неосторожной форме вины[320].

Процесс установления возможной формы вины нарушения правил эксплуатации средств и правил доступа к объектам, перечисленным в диспозициях ч. 1 ст. 274 и ч. 3 ст. 274^1 УК РФ, на наш взгляд, должен осуществляться следующим образом. Рассматриваемые составы преступлений являются материальными, что обуславливает необходимость наложения при анализе субъективной стороны состава преступления всех признаков форм вины, указанных в ст.ст. 25, 26 УК РФ.

---

[317] Апелляционное определение Самарского областного суда от 08.02.17 г. по делу № 22-627/2017 // ГАС «Правосудие». URL: http://oblsud.sam.sudrf.ru/ (дата обращения: 13.07.17).

[318] См.: Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. В. М. Лебедев. 14-е изд., перераб. и доп. М.: Юрайт, 2014. С. 810; Уголовное право России. Особенная часть: Учебник / Под ред. Ф. Р. Сундурова, М. В. Талан. М.: Статут, 2012. С. 624; Уголовное право РФ. Особенная часть: Учебник / Л. В. Иногамова-Хегай и др.; Под ред. Л. В. Иногамовой-Хегай. М.: НИЦ ИНФРА-М, 2013. С. 248; Уголовное право Российской Федерации. Общая и Особенная части: Учебник / Под ред. А. И. Чучаева. М.: Контракт, 2016. С. 567; Уголовное право. Особенная часть: Учебник / Отв. ред. И. Я. Козаченко, Г. П. Новоселов. 5-е изд., изм. и доп. М.: Норма : НИЦ ИНФРА-М, 2013. С. 723; Дворецкий М. Ю. Указ. соч. С. 130; Наумов А. В. Российское уголовное право. Курс лекций. В двух томах. Т. 2. Особенная часть. М.: Юрид. лит., 2004. С. 568.

[319] См.: Преступления в сфере компьютерной информации: квалификация и доказывание. Учебное пособие / Гаврилин Ю.В., Головин Ю. В., Кузнецов А. В., Толстухина Т. В. М.: Книжный мир, 2003. С. 53; Уголовное право. Особенная часть: Учебник. Издание второе исправленное и дополненное / Под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева. М.: Контракт, 2008. С. 561; Полный курс уголовного права: Преступления против общественной безопасности. В 5-ти томах. Т. 4 / Под ред.: А. И. Коробеева. С.-Пб.: Юрид. центр Пресс, 2008. С. 402; Зинина У. В. Указ. соч. С. 95.

[320] См.: Уголовное право. Особенная часть: Учебник. Издание второе исправленное и дополненное / Под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева. М.: Контракт, 2008. С. 552.

На первый взгляд, интеллектуальные моменты рассматриваемых составов преступлений характеризуются *осознанием* своих действий или бездействий в виде нарушения *правил* как факта общественно опасного явления. Субъект преступления должен осознавать, что они *существуют*, *знать* их, *понимать*, что их нарушение способно повлечь общественно опасные последствия. На наш взгляд, лицо в рамках рассматриваемых составов преступлений всегда осуществляет эксплуатацию и доступ к компьютерной информации *правомерно* (в отличие от деяния, описанного в ч. 1 ст. 272 УК РФ), будучи 1) наделенным правами и соответствующими обязанности по отношению к работе с компьютерной информацией, либо 2) должностным лицом в силу служебного положения, либо 3) по договору.

Исполнитель преступления также должен предвидеть *возможность* наступления последствий в определенном законодателем в ч. 1 ст. 274 УК РФ *виде* и *размере*. Так, в качестве их видов в составе перечисляются уничтожение, блокирование, модификация и копирование, которые должны предвидеться. Также им должны предвидеться наступление последствий в определенном размере – крупном ущербе (свыше одного миллиона рублей). При квалификации по ч. 3 ст. 274^1 УК РФ следует учесть, что субъектом должно предвидеться возможность наступления последствий только одного вида: в виде вреда КИИ РФ.

При прямом умысле предвидение, характеризуясь неизбежностью их наступления, на наш взгляд, не может быть свойственно указанному деятелю. Об этом свидетельствует установленный законодателем максимальный размер санкции за совершаемые деяния в виде лишения свободы до 2 лет по ч. 1 ст. 274 УК РФ и до 6 лет – по ч. 3 ст. 274^1 УК РФ. Так, в ч. 1 ст. 272 УК РФ, последствия не выражаются такой высокой степенью общественной опасности (последствия выражены только в виде уничтожения, блокирования, модификации либо копировании компьютерной информации), по сравнению с ч. 1 ст. 274 УК РФ, в которой указывается на наступление помимо тех же последствий еще и причинение крупного ущерба. Более того, трудно предположить, что субъект, будучи наделенным специальными правами в связи с тем, что он является

специальным субъектом преступления в силу своего служебного положения или иных обстоятельств (что уже повышает степень общественной опасности его деяния), намеренно причиняющий вред охраняемым законом интересам в крупном размере, будет нести ответственность в равном размере с субъектом, неправомерно осуществляющим уничтожение, блокирование, модификацию или копирование компьютерной информации либо воздействие на КИИ.

Кроме того, сам по себе признак «нарушения правил» обычно характеризует также неосторожную форму вины. Субъекты, осуществляющие эксплуатацию указанных в законе систем и информации и доступ к ним, могут намеренно нарушать правила, но при любом исходе они для него остаются *нежелательными* (волевой момент), тем более в каком-то размере. В том случае, если специалист, который нарушает правила, для уничтожения информации и в определенном крупном ущербе, относится к ним как к желательным, то сфера его интереса должна лежать, как нам представляется, за пределами охраняемого уголовным законом объекта в виде безопасности компьютерной информации.

Иными словами, субъективная сторона деятеля при нарушении правил характеризуется расчетом на их предотвращение с надеждой на себя или другие объективные факторы (нежеланием наступления последствий), либо им они должны были и могли предвидеться (при должной внимательности и предусмотрительности) в силу наличия профессиональных качеств (как специалиста), что характеризует уже небрежность. Небрежность, будучи крайней формой вины, характерна именно для субъектов, которые должны и могут знать о возможности наступления негативных последствий в силу разных объективных причин.

Таким образом, преступления, ответственность за которые установлена ч. 1 ст. 274 УК РФ и ч. 3 ст. 274^1 УК РФ, характеризуются только неосторожной формой вины. По этому же основанию, как нами отмечалось, характер своего деяния субъектом не должен осознаваться, как устанавливалось на первый взгляд, а должен пониматься.

В качестве признаков субъективной стороны основных составов рассматриваемых преступлений могут выступать мотивы и цели совершения преступления того или иного преступления.

Мотив – это осознанное побуждение, которое приводит человека к удовлетворению своих потребностей (физиологический, общих) путем совершения преступления. Установление мотива дает ответ на вопрос, почему совершается преступление[321]. *Цель* – это образ результата, который субъект стремится получить в процессе совершения преступления. Установление цели позволяет ответить на вопрос, для чего совершается преступление. Некоторыми авторами корыстная заинтересованность называется в качестве возможной цели совершения преступлений против безопасности компьютерной информации, однако, являясь уже квалифицирующим признаком составов преступлений против безопасности компьютерной информации, будет нами рассмотрена в последующем параграфе.

По содержанию субъективных признаков составы преступлений против безопасности компьютерной информации могут быть связаны с определенным видом мотивации (к примеру, корыстная заинтересованность в ч. 2 ст. 272 УК РФ, где она названа в качестве квалифицирующего признака). В то же время в основных составах рассматриваемых преступлений не содержатся указания на какой-либо определенный мотив преступления. Следовательно, законодатель допускает совершение предусмотренных ими деяний при наличии *любого* мотива, при этом лишь корыстная заинтересованность является признаком квалифицированного состава (см., напр., ч.ч. 2 ст. 272, 273 УК РФ).

Как справедливо отмечается в литературе, мотивы и цели, если они не указаны в основных составах преступления преступлений, на квалификацию не влияют[322]. Изучение практики показывает, что наиболее распространенными мотивами преступлений против безопасности компьютерной информации являются месть, зависть, хулиганские побуждения, желания испортить кому-либо

---

[321] См.: Волков Б. С. Указ. соч. С. 32-34.

[322] См.: Преступления в сфере компьютерной информации: квалификация и доказывание. Учебное пособие / Гаврилин Ю.В., Головин Ю. В., Кузнецов А. В., Толстухина Т. В. М.: Книжный мир, 2003. С. 27.

деловую репутацию или скрыть другое преступление, «спортивный» интерес[323], обида, неприязнь, мести из-за невыплаты заработной платы, бескорыстные побуждения, обусловленные стремлением безвозмездного распространения среди неограниченного круга лиц программного обеспечения, личная неприязнь, связанная с увольнением из цели воздействия на принятие решения бывшим работодателем: изменение основания увольнения в трудовой книжке работника, цели в виде неосновательного обогащения[324] и др.[325]

§ 4. Уголовно-правовая характеристика субъекта преступления и его установление в ходе квалификации посягательств против безопасности компьютерной информации

Согласно ст. 19 УК РФ уголовной ответственности подлежит только вменяемое физическое лицо, достигшее к моменту совершения преступления возраста, установленного УК РФ. В уголовном законе отсутствует понятие *вменяемости*, однако имеется противоположное ему определение, характеризующееся двумя критериями: медицинским (биологическим) и юридическим (психологическим). Таким образом, под вменяемостью следует понимать способность лица осознавать фактический характер и общественную опасность своего действия или бездействия и руководить ими[326].

По статистике Судебного департамента при ВС РФ за 2012-2016 гг. по рассматриваемым преступлениям признано невменяемыми в 2016 г. – 0 чел., в

---

[323] См.: Указ. соч. С. 28.

[324] Приговор Альметьевского городского суда Республики Татарстан от 24.05.12 г. по делу № 1-294 // ГАС «Правосудие». URL: http://almetevsky.tat.sudrf.ru/ (дата обращения: 17.07.17).

[325] Приговор Ново-Савиновского районного суда г. Казани Республики Татарстан от 20.05.15 г. по делу № 1-14/15 // ГАС «Правосудие». URL: http://novo-savinsky.tat.sudrf.ru (дата обращения: 13.07.17); Приговор Набережночелнинского городского суда Республики Татарстан от 24.10.13 г. по делу № 1-1196/13 // ГАС «Правосудие». URL: http://naberezhno-chelninsky.tat.sudrf.ru/ (дата обращения: 17.07.17); Приговор Магаданского городского суда Магаданской области от 18.01.17 г. по делу № 1-58/2017 // ГАС «Правосудие». URL: http://magadansky.mag.sudrf.ru/ (дата обращения: 18.07.17); Приговор Советского районного суда г. Казани Республики Татарстан от 02.07.14 г. по делу № 1-437/2014 // ГАС «Правосудие». URL: http://sovetsky.tat.sudrf.ru/ (дата обращения: 13.07.17); Приговор Железнодорожного районного суда г. Самары Самарской области от 29.12.15 г по делу № 1-350/2015 // ГАС «Правосудие» (http://zheleznodorozhny.sam.sudrf.ru/ (дата обращения: 17.07.17).

[326] См.: Практикум по уголовному праву России / Под ред. Ф. Р. Сундурова, М. В. Талан, И. А. Тарханова. М.: Статут, 2014. С. 55.

2015 г. – 1, в 2014 г. – 2, в 2013 г. – 0, в 2012 г. – 0[327]. За период с 2012-2016 гг. только одному лицу, страдающему психическим расстройствами, не исключающим вменяемость лица, определено лечение, в 2016 г. не имелось таких лиц, в 2015 г. судом определено лечение у врача-психиатра 1 человеку, в 2014 г. – 0, в 2013 г. – 0, в 2012 г. – 2[328].

Субъектом преступления является только *физическое лицо*. Физическими лицами в теории права признаются все граждане, иностранцы и лица без гражданства[329].

Среди лиц, осуществляющих посягательства против безопасности компьютерной информации, наибольшую долю занимают лица мужского пола. Лица женского пола составляют лишь незначительную ее часть (см. Приложение 5). Порядка 70% осужденных имеют высшее профессиональное либо среднее профессиональное образование (см. Приложение 6).

Достижение *возраста уголовной ответственности* является обязательным условием наступления уголовной ответственности. По общему правилу уголовной ответственности подлежит лицо, достигшее ко времени совершения преступления 16 лет (ч. 1 ст. 20 УК РФ). Исключения из общего правила составляют составы преступлений, перечисленные в ч. 2 ст. 20 УК РФ. Представляется, что такие преступления носят либо высокую степень общественной опасности или в полной мере могут осознаваться несовершеннолетнем лицом. К сожалению, единого критерия снижения возраста уголовной ответственности сегодня установить не удается[330]. Одним из дискуссионных признаков основных составов преступлений против безопасности компьютерной информации является возраст наступления уголовной ответственности. Имеющиеся в науке доводы о необходимости введения

---

[327] Данные судебной статистики Судебного департамента при ВС РФ // URL: http://www.cdep.ru/index.php?id=79 (дата обращения: 18.07.17).

[328] Данные судебной статистики. Там же.

[329] См.: Общая теория государства и права. В 3-х т. Т. 2. Право: Академ. курс / М. Н. Марченко, С. Н. Бабурин и др.; Отв. ред. М. Н. Марченко. 4-е изд., перераб. и доп. М.: Норма : НИЦ ИНФРА-М, 2013. С. 668.

[330] Например, тяжело представить осознание лицом в возрасте от 14 до 16 лет цели нарушения мирного сосуществования народов (ст. 361 УК РФ). Н. К. Семернева вовсе называет градацию возраста (ч. 2 ст. 20 УК РФ) преступлений против мира и безопасности человечества неприемлемой. См., также: Семернева Н. К. Указ. соч. С. 118.

уголовной ответственности за анализируемые преступления с 14 лет весьма убедительны[331]. Однако уголовное право, будучи крайней мерой правового регулирования отношений, должно вступать в такую регуляцию только в исключительных случаях. На наш взгляд, методы других правовых институтов не исчерпаны. Данное положение касается, прежде всего, административно-правового регулирования таких правонарушений. Отсутствуют и свидетельства о массовости компьютерной преступности среди несовершеннолетних и их крайней общественной опасности. Кроме того, согласно статистическим сведениям доля несовершеннолетних лиц, осужденных за указанных преступлений, незначительна (см. *Приложение 7*)[332]. По данным статистики 2012-2016 гг. среди лиц, осужденных за преступления подобного рода, в 2014 году было осуждено только одно лицо в возрасте от 16-17 лет ранее не судимое и одно лицо в возрасте 16-17 лет в 2016 г.[333] При таких обстоятельствах мы разделяем мнение ученых, считающих снижение возраста уголовной ответственности за данные преступления неприемлемым[334].

В теории уголовного права субъект преступления принято разделять на *общий* и *специальный*. Под специальным субъектом преступления понимается исполнитель преступления, обладающий наряду с основными признаками дополнительными (факультативными) признаками (возраст, пол, профессия, отношения к потерпевшему, служебное положение и др.)[335].

Схожие особенности, характеризующие деятеля, в т.ч. с криминологической стороны, можно вывести из толкования *каждой* общей нормы, предусматривающей ответственность за все исследуемые нами виды преступлений. Так, в ч. 1 ст. 272 УК РФ и ч. 2 ст. 274^1 УК РФ, нам представляется, говорится о деятеле, *не обладающем правом доступа к компьютерной информации*. Такое обстоятельство имеет важное значение для установления

---

[331] См.: Айсанов Р. М. Указ. соч. С. 105; Шарков А. Е. Указ. соч. С. 149; Карпов В. С. Указ. соч. С. 127.
[332] Данные судебной статистики. Там же.
[333] Там же.
[334] См.: Баштовая А. Н. Уголовная ответственность и наказание несовершеннолетних // Юрист-Правоведъ. 2008. № 3. С. 36-39; Карпов В. С. Указ. соч. С. 127; Степанов-Егиянц В. Г. Указ. соч. С. 214.
[335] См.: Семернева Н. К. Указ. соч. С. 120.

также и формы вины субъекта[336]. 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 характеризующей 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 (напр., ст.ст. 124, 192, 215, 216, 217 УК РФ и др.). Однако имеется и противоположная точка зрения, согласно которой субъект преступления, ответственность за которое установлено ст. 274 УК РФ, является общим[337]. Такая позиция нами не разделяется.

Вместе с тем нельзя говорить, что каждый состав преступления против безопасности компьютерной информации характеризуется указанием на специальный субъект преступления. Правильное установление признаков специального субъекта имеет значение при установлении соответствия между деянием и составами преступлений против безопасности компьютерной информации, с учетом их квалифицированных признаков. Так, в ч. 3 ст. 272, ч. 2 ст. 273, ч. 4 ст. 274[1] УК РФ указывается на совершении рассматриваемых преступлений лицом с использованием своего служебного положения.

При квалификации преступлений против безопасности компьютерной информации важно определять все обстоятельства, характеризующие признаки субъекта преступления. Так, по одному из дел органами предварительного следствия А. обвинялся в нарушении правил эксплуатации средств хранения и

---

[336] См.: Дворецкий М. Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания: Монография. Тамбов: Изд-во ТГУ им. Г. Р. Державина, 2003. С. 136.

[337] См.: Степанов-Егиянц В. Г. Указ. соч. С. 306; Волеводз А. Г. Волеводз А. Г. Противодействие к компьютерным преступлениям: правовые основы международного сотрудничества / А. Г. Волеводз. М.: Юрлитинформ, 2002. С. 81.

передачи охраняемой компьютерной информации, повлекшее копирование компьютерной информации, причинившее крупный вред (ч. 1 ст. 274 УК РФ). Правоприменителем установлено, что А. работал и занимал различные должности в отделе технической поддержки ОС UNIX ООО «Приват Трейд» (потерпевшее лицо), также с А. были заключены соглашения о сохранении служебной и коммерческой тайн, о конфиденциальности для работников ООО «Приват Трейд», и он был ознакомлен с должностной инструкцией по должности ведущего системного администратора ОС UNIX. Изложенные обстоятельства позволяют утверждать о возложении на А. конкретных обязанностей по соблюдению правил.

Законодателем в 2011 г. из конструкции ст. 274 УК РФ исключены слова «лицом, имеющим доступ»[338]. Наличие доступа к техническим средствам необходимо было трактовать в узком смысле. Таким лицом должны были признаваться субъекты, на законных основаниях работающие с техническими средствами. Поэтому, анализируя ст. 274 УК РФ в новой редакции, необходимо задаться вопросом: возможно ли нарушение указанных в диспозиции ст. 274 УК РФ правил лицом, не имеющим доступа к техническим средствам? Нам представляется, что наличие такого признака в диспозиции было излишним. В связи с тем, что субъект преступления, ответственность за которое предусмотрено ст. 274 УК РФ, специальный, из ее толкования подразумевается, что у лица имеется доступ к работе с техническими средствами.

Таким образом, 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,

---

[338] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации : федер. закон Рос. Федерации от 7 дек. 2011 г. № 420-ФЗ : принят Гос. Думой Федер. Собр. Рос. Федерации 17 нояб. 2011 г. : одобр. Советом Федерации Федер. Собр. Рос. Федерации 29 нояб. 2011 г. // Собр. законодательства Рос. Федерации. 2011. № 50, ст. 7362.

может нести лишь специальный субъект, т.е. лицо, обладающее знаниями определенных правил эксплуатации и правил доступа.

§ 5. Особенности уголовно-правовой оценки содеянного при наличии квалифицирующих и особо квалифицирующих признаков составов рассматриваемых составов преступлений

Как уже отмечалось ранее, квалифицированными и особо квалифицированными видами составов преступлений против безопасности компьютерной информации являются конструкции, где указывается на отягчающие и особо отягчающие уголовную ответственность обстоятельства. Они предусмотрены в иных частях уголовно-правовой нормы, предусматривающей данный вид преступления.

Следует обратить внимание, что указания на признаки, смягчающие уголовную ответственность, среди характеристик всех видов преступлений против безопасности компьютерной информации отсутствуют. Иными словами, привилегированных составов среди них нет.

Признаками, преобразующими основной состав преступления против безопасности компьютерной информации в квалифицируемый или особо квалифицируемый, являются как объективные, так и субъективные признаки деяния. Представляется, что их можно разделить на три группы: *объективные* квалифицирующие признаки: причинение крупного ущерба, тяжкие последствия либо угроза их наступления; *субъективный* квалифицирующий признак: корыстная заинтересованность; *объективно-субъективные* квалифицирующие признаки: использование служебного положения, совершение деяния группой лиц по предварительному сговору либо организованной группы.

Квалифицирующие признаки анализируемых в данной работе преступлений в виде совершения их группой лиц по предварительному сговору или организованной группой лиц будут нами рассмотрены в следующей главе.

Причинение крупного ущерба как признак объективный стороны состава преступления, как возможного последствия признается в качестве квалифицирующего признака при неправомерном доступе к компьютерной информации (ч. 2 ст. 272 УК РФ) и создании, использовании и распространении вредоносных компьютерных программ (ч. 2 ст. 273 УК РФ). При этом оно преобразует деяние в виде создания, использования и распространения ВКП (части 2 и 3 ст. 273 УК РФ) в квалифицирующий состав, описанный по материальному типу, что обусловливает возможность совершения указанного преступления по легкомыслию. Это обязывает правоприменителя устанавливать наличие причинно-следственной связи между указанным деянием и наступившими последствиями в виде крупного ущерба.

Согласно второму примечанию к ст. 272 УК РФ, крупным ущербом признается ущерб, сумма которого превышает один миллион руб. Такой признак является конкретизированным (аутентичным). Что обязывает правоприменителя доказать и указать в принимаемом акте, что именно в результате совершения преступного деяния вредные последствия наступили в указанном объеме[339].

Следует согласиться с тем, что крупный ущерб может оказаться в любой сфере: материальной, физической, моральной, политической, правовой [340] . Например, У. блокирована и удалена информация, находящаяся на Интернет-ресурсе, вследствие чего причинен имущественный ущерб, связанный с восстановлением блокированной, модифицированной и удаленной информации[341].

Оценка причиненного ущерба должна осуществляться на момент причинения вреда. Как справедливо указывает Н. А. Лопашенко, «во внимание должен приниматься тот ущерб, который был реально нанесен собственнику, т.е. не средней стоимостью, а реально тот, который был уплачен за это имущество

---

[339] Об этом же говорится в п. 19 постановления Пленума Верховного Суда Российской Федерации от 29 ноября 2016 г. № 55 «О судебном приговоре», в котором указывается, что признавая подсудимого виновным в совершении преступления по признакам, относящимся к оценочным категориям (например, тяжкие последствия), «суд не должен ограничиваться ссылкой на соответствующий признак, а обязан привести в описательно-мотивировочной части приговора обстоятельства, послужившие основанием для вывода о наличии в содеянном указанного признака».

[340] См.: Смирнова Т. Г. Указ. соч. С. 82

[341] Приговор Ново-Савиновского районного суда г. Казани Республики Татарстан от 18.04.16 г. по делу № 1-160/2016 // ГАС «Правосудие». URL: http://novo-savinsky.tat.sudrf.ru (дата обращения: 13.07.17).

потерпевшим» [342] . Такое положение актуально и к рассматриваемым преступлениям против безопасности компьютерной информации. Размер причиненного ущерба может устанавливаться, к примеру, на основании проведенной бухгалтерской экспертизы.

Тяжкие последствия либо угроза их наступления являются квалифицирующими или особо квалифицирующими признаками неправомерного доступа к компьютерной информации (ч. 4 ст. 272 УК РФ), создания, использования и распространения ВКП (ч. 3 ст. 273 УК РФ) и нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ч. 2 ст. 274 УК РФ). Признак тяжких последствий – в ч. 5 ст. 274^1 УК РФ.

Тяжкие последствия предполагают причинение такого размера ущерба, которое является существенно больше крупного ущерба и значимее для потерпевшей стороны. Характер тяжести последствий в указанных нормах законодателем не раскрывается, поэтому такой признак называется оценочным. Оценочный признак позволяет правоприменителю в полной мере учесть все обстоятельства дела при квалификации преступления.

Тяжесть последствий может быть однородна преступлениям против безопасности компьютерной информации, иными словами, при квалификации ее необходимо искать в сфере тех же общественных отношений, на охрану которых направлены уголовно-правовые нормы, предусмотренные ст.ст. 272-274^1 УК РФ. Однородными следует признавать потерю исключительно важной информации, наличие которой обеспечивает функционирование компьютерных устройств, программ, систем и сетей, возможность причинения вреда КИИ РФ.

В качестве тяжких последствий могут рассматриваться причинение крупного материального ущерба пользователям компьютерной техники, длительную остановку работы предприятия или учреждения, несчастные случаи с людьми

[342] Лопашенко Н. А. Посягательства на собственность: монография / Н. А. Лопашенко. М.: Норма : ИНФРА-М, 2012. С. 167.

(причинение тяжкого вреда здоровью или смерти хотя бы одному человеку)[343]. Некоторыми исследователями к тяжким последствиям относятся причинение легкого вреда здоровью, причинение средней тяжести вреда здоровью[344]. На наш взгляд, иные виды вреда здоровью отличные от тяжких – средней тяжести, легкий вред – по самой терминологии к тяжким последствия относить нельзя. Также в литературе к тяжким последствиям рассматриваемых преступлений относят причинение средней тяжести вреда здоровью *двум и более лицам*, *массовое* причинение легкого вреда здоровью людей [345] . Однако, как справедливо указывается по этому вопросу в литературе, «складывать несколько отдельных последствий и затем считать эту сумму тяжким последствием нет оснований»[346].

Когда в норме имеется указание не на реально наступившие последствия, а на *угрозу наступления указанных последствий,* в уголовно-правовой теории такие составы преступлений получили название составов опасности[347]. Поэтому ч. 4 ст. 272, ч. 3 ст. 273, ч. 2 ст. 274 УК РФ мы можем отнести также к составам конкретной опасности, которые необходимо признавать оконченными с момента наступления *реальной* угрозы тяжких последствий (усеченные составы преступлений).

Угроза наступления последствий – это реальная возможность наступления последствий, т.е. для их вменения должны быть четкие объективные основания к их наступлению. Фактическое наступление последствий не влияет на квалификацию преступления. Так, по одному из дел установлено, что в результате сбоя программного обеспечения предприятия, а именно удаления компьютерной программы для автоматического получения заявок от покупателей, возникла угроза штрафных санкций от покупателей в связи с несвоевременной поставкой продукции покупателям, а также необходимость привлечения дополнительных

---

[343] См.: Полный курс уголовного права: Преступления против общественной безопасности. В 5-ти томах. Т. 4 / Под ред.: А. И. Коробеева. С.-Пб.: Юрид. центр Пресс, 2008. С. 398.
[344] См.: Там же.
[345] См.: Ляпунов Ю. И., Пушкин А. В. Преступления в сфере компьютерной информации // Уголовное право. Особенная часть / Под ред. Н. И. Ветрова, Ю. И. Ляпунова. М.: Новый Юрист, КноРус, 1998. С. 559.
[346] Семернева Н. К. Указ. соч. С. 66.
[347] См.: Корнеева А. В. Указ. соч. С. 26.

трудовых ресурсов сверхурочно для ручной обработки заявок[348].

Также необходимо принимать во внимание, что при квалификации деяний по рассматриваемому признаку необходимо раскрывать, какие конкретно тяжкие последствия могли наступить для потерпевших от инкриминируемых обвиняемому деяний, а не ограничиваться абстракцией в виде констатирования. К примеру, по указанным основаниям Тверской районный суд г. Москвы постановил вернуть прокурору одно из уголовных дел[349].

Корыстная заинтересованность является квалифицирующим признаком составов неправомерного доступа к компьютерной информации (ч. 2 ст. 272 УК РФ) и создания, использования и распространения вредоносных компьютерных программ (ч. 2 ст. 273 УК РФ).

Под корыстной заинтересованностью согласно разъяснениям, данным ВС РФ, понимается стремление путем совершения неправомерных действий получить для себя или других лиц выгоду имущественного характера либо избавиться от материальных затрат (освобождение от каких-либо имущественных затрат, погашения долга, оплаты услуг, уплаты налогов и т.п.)[350]. Так, Советским районным судом г. Казани лицу вменен признак корыстной заинтересованности в связи с тем, что он осуществил неправомерный доступ к компьютерной информации, повлекший ее блокирование. После за разблокирование потребовал от собственника информации денежную сумму в размере 22 000 руб.[351]

Корыстная мотивация может выражаться в целях безвозмездного использования всемирной компьютерной сети Интернет[352], неосновательного

---

[348] Приговор Набережночелнинского городского суда Республики Татарстан от 24.10.13 г. по делу № 1-1196/13 // ГАС «Правосудие». URL: http://naberezhno-chelninsky.tat.sudrf.ru/ (дата обращения: 17.07.17).

[349] Апелляционное постановление Московского городского суда от 15.06.16 г. по делу № 10-7792/16 // ГАС «Правосудие». URL: https://www.mos-gorsud.ru/ (дата обращения 18.07.17).

[350] О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий : постановление Пленума Верховного Суда РФ от 16 окт. 2009 г. № 19 // Рос. газ. 2009. №5031 (207).

[351] Постановление Советского районного суда города Казани Республики Татарстан от 11.07.16 г. № 1-416/2016 // ГАС «Правосудие». URL: http://sovetsky.tat.sudrf.ru/; (дата обращения: 13.07.17).

[352] Приговор Альметьевского городского суда Республики Татарстан от 15.03.13 г. по делу № 1-137/2013 // ГАС «Правосудие». URL: http://almetevsky.tat.sudrf.ru/ (дата обращения: 17.07.17); Приговор Арского районного суда Республики Татарстан от 27.03.13 г. по делу № 1-16/13 // ГАС «Правосудие». URL: http://arsky.tat.sudrf.ru/ (дата обращения: 13.07.17); Приговор Менделеевского районного суда Республики Татарстан от 15.10.12 по делу № 1-89/12 // ГАС «Правосудие». URL: http://mendeleevsky.tat.sudrf.ru/ (дата обращения 18.07.17).

обогащения[353], хищении денежных средств[354] и др. Корыстный мотив, на наш взгляд, незаслуженно упущен при конструировании состава неправомерного воздействия на КИИ РФ. Представляется, что доля таких преступлений будет составлять значительную часть среди именуемых посягательств и поэтому целесообразно для включения в качестве квалифицирующего признака в ч. 4 ст. 274^1 УК РФ.

Использование лицом своего служебного положения является квалифицирующим признаком составов неправомерного доступа к компьютерной информации, ответственность за которое предусмотрена ч. 3 ст. 272 УК РФ; создания, использования и распространения вредоносных компьютерных программ, ответственность за которое предусмотрена ч. 2 ст. 273 УК РФ; а также составов неправомерного воздействия на КИИ РФ, ответственность за которые предусмотрена ч.1-3 ст. 274^1 УК РФ.

При использовании лицом в преступной деятельности своего служебного положения нарушаются общественные отношения, обеспечивающие интересы службы, являющиеся обязательным дополнительным объектом уголовно-правовой охраны. Признак использования лицом служебного положения должен вменяться лицам, на законных основаниях работающим с компьютерной техникой или обслуживающим ее. Такими могут быть признаны программисты, системные администраторы, специалисты отделов автоматизированных систем управления, работники операторов связи и т.д. Например, В. признан виновным по ч. 2 ст. 138 УК РФ и ч. 3 ст. 272 УК РФ в том, что, работая в должности специалиста в одной из телефонных компаний, по просьбе предоставил информацию по детализации телефонных соединений абонента, переслав ее на электронную почту[355]. Х. вменен квалифицирующий признак совершения преступления с использованием своего

---

[353] Приговор Альметьевского городского суда Республики Татарстан от 24.05.12 г. по делу № 1-294 // ГАС «Правосудие». URL: http://almetevsky.tat.sudrf.ru/ (дата обращения: 17.07.17); Приговор Набережночелнинского городского суда Республики Татарстан от 05.12.16 г. по делу № 1-1467 // ГАС «Правосудие». URL: http://naberezhno-chelninsky.tat.sudrf.ru/ (дата обращения: 17.07.17).

[354] Приговор Промышленного районного суда г. Самары Самарской области от 22.04.16 г. по делу № 1-219/2016 // ГАС «Правосудие». URL: http://promyshleny.sam.sudrf.ru/ (дата обращения: 18.07.17).

[355] Апелляционное постановление Самарского областного суда от 16.01.17 г. по делу № 22-190/2017 // ГАС «Правосудие». URL: http://oblsud.sam.sudrf.ru/ (дата обращения: 13.07.17).

служебного положения, ответственность за которое предусмотрено по ч. 3 ст. 272 УК РФ, в силу того, что он был наделен правом доступа к компьютерным программам и распоряжения находящимися на лицевых счетах абонентов денежными средствами, являясь представителем этой организации[356].

Справедливо отмечается, что нельзя вменять указанный квалифицированный признак лицам, по служебной деятельности не имеющим непосредственное отношение к доступу к компьютерной технике (уборщикам производственных и служебных помещений, специалистам, обслуживающим вентиляционные установки, охранникам и др.)[357].

Отдельного внимания заслуживает законодательная конструкция ст. 274^1 УК РФ, являющаяся первой в УК РФ составом преступления, объединяющим в одной из своих частей (а именно в части 2) две общие нормы (ст. 272 и 273 УК РФ) использовав союз «в том числе».

В ч. 2 ст. 274^1 УК РФ законодателем в качестве квалифицирующего признака предусмотрена менее строгая норма об ответственности за неправомерный доступ к компьютерной информации (ч. 1 ст. 272 УК РФ – преступление небольшой тяжести) в отличие от более строгой, предусматривающей ответственность за неправомерный оборот ВКП (ч. 1 ст. 273 УК РФ – преступление средней тяжести). Такой вывод обосновывает необходимость перестановки местами частей 1 и 2 ст. 274^1 УК РФ и исключения из ч. 2 ст. 274^1 УК РФ в нынешней редакции конструкции, предусматривающей ответственность за оборот ВКП, предназначенных для неправомерного воздействия на КИИ РФ. Указанные положения позволили бы восстановить логику построения уголовно-правовой нормы.

---

[356] Апелляционное постановление Самарского областного суда от 20.10.14 г. по делу № 22-4759/14 // ГАС «Правосудие». URL: http://oblsud.sam.sudrf.ru/ (дата обращения: 13.07.17).

[357] См.: Уголовное право России. Особенная часть: Учебник / Под ред. Ф. Р. Сундурова, М. В. Талан. М.: Статут, 2012. С. 620.

Глава 4. Применение специальных правил квалификации преступлений против безопасности компьютерной информации

§ 1. Понятие и квалификация неоконченной преступной деятельности, направленных против безопасности компьютерной информации

Согласно ч. 1 ст. 29 УК РФ, преступление признается оконченным, если в совершенном деянии содержатся все признаки состава преступления, предусмотренного УК РФ. Стадии совершения преступлений против безопасности компьютерной информации, предшествующие признанию преступления в качестве оконченного, образуют предварительную преступную деятельность, включающую приготовление к преступлению и покушение на преступление (ч. 2 ст. 29 УК РФ). Согласно статистике, доля прерванной преступной деятельности по независящим от лица обстоятельствам среди всех рассматриваемых нами преступлений идет на спад. Так, в 2013 г. доля таких преступлений составляла 8,2%, в 2014 г. – 5,5%, в 2015 г. – 4,7%, в 2016 г. – 1,6% (см. *Приложение 9*).

Приготовлением к преступлению признается умышленное создание условий для совершения преступления, если при этом преступление не было доведено до конца по не зависящим от этого лица обстоятельствам. В качестве приготовительных действий закон называет приискание соучастников преступления и сговор на совершение преступления.

Согласно ч. 2 ст. 30 УК РФ, уголовная ответственность наступает за приготовление только к тяжким и особо тяжким преступлениям. Некоторые из рассматриваемых в диссертации преступлений, судя по санкциям, предусмотренным основными составами (ч. 1 ст. 272, ч. 1 ст. 274), относятся к категории небольшой тяжести, поскольку максимальное наказание за их совершение не превышает двух лет лишения свободы. Деяние, признаки основного состава которого изложены в ч. 1 ст. 273, признается преступлением средней тяжести, поскольку максимальный срок наказания в виде лишения свободы не превышает четырех лет лишения свободы. Следовательно, совершение

приготовительных действий к преступлениям, ответственность за которые предусмотрена ч. 1 ст. 272, ч. 1 ст. 273 и ч. 1 ст. 274, не являются уголовно-наказуемыми деяниями в силу ч. 2 ст. 30 УК РФ.

В соответствии с ч. 3 ст. 30 УК РФ «покушением на преступление признаются умышленные действия (бездействие) лица, непосредственно направленные на совершение преступления, если при этом преступление не было доведено до конца по не зависящим от этого лица обстоятельствам». Таким образом, основным отличием приготовления от покушения на преступление является то, что в приготовительных действиях отсутствуют признаки объективной стороны соответствующего состава преступления. По общему правилу невозможно покушение на формальные составы преступлений. Состав создания, использования и распространения ВКП (ст. 273), в том числе то же деяние, направленное на КИИ РФ (ч.1 ст. 274^{1}), являются по конструкциям объективной сторон их составов формальными. Исключением из общего правила являются случаи наличия разрыва во времени между началом деяния и его окончанием либо исполнение лицом сложных, неодноактных действий [358]. В качестве таких деяний необходимо рассматривать «создание» и «распространение» ВКП или компьютерной информации подобного рода, на которые имеются указания в диспозициях ч. 1 ст. 273 и ч. 1 ст. 274^{1} УК РФ.

Момент окончания создания ВКП нами в достаточной мере обоснован в предыдущей главе настоящей работы. Поэтому различные стадии (этапы) *создания* ВКП или иной компьютерной информации, исключающие возможность их использования по причинам, не зависящим от виновного лица, следует квалифицировать как покушение на преступление по ч. 3 ст. 30 и ст. 273 УК РФ.

Предложенная нами классификация способов распространения на активный и пассивный имеет определенное значение для квалификации неоконченного распространения ВКП. Если для активного распространения ВКП важен момент ее получения другим лицом, то для пассивного оно не имеет никакого значения. Таким образом, пассивное распространение состоит из меньшего количества

[358] См.: Сабитов Р. А. Указ. соч. С. 89; Корнеева А. В. Указ. соч. С. 102.

совершаемых действий. Вместе с тем покушение возможно на оба способа распространения вредоносных компьютерных программ.

Установление формы и вида умысла преступления против безопасности компьютерной информации по правилам, определенным в § 3 главы 3 настоящей работы, значимо для квалификации преступления в качестве неоконченного. Так, приготовление и покушение на совершение всех рассматриваемых нами видов преступлений, являющиеся материальными, возможно только с прямым умыслом.

Создание или использование лицом ВКП либо иной компьютерной информации подобного рода для неправомерного доступа к охраняемой законом компьютерной информации образует изготовление им средства совершения или создание условий для совершения преступления, т.е. приготовительную преступную деятельность. В таких случаях приготовление к преступлению полностью совпадает с составом преступления, предусмотренным ст. 273 УК РФ, и перечисленные действия лица при их полном окончании необходимо квалифицировать по совокупности преступлений, ответственность за которые предусмотрена соответствующими частями ст.ст. 272 и 273 УК РФ. Иными словами, каждая последующая стадия совершения преступления поглощает все предыдущие, и они не требуют самостоятельной уголовно-правовой оценки. Так, Советским районным судом г. Казани действия У., который использовал вредоносную компьютерную программу DUBrute, предназначенную для нейтрализации средств защиты компьютерной информации, смог получить логин и пароль от сервера для дальнейшего осуществления удаленного несанкционированного доступа в систему, правильно квалифицированы по совокупности преступлений[359]. Однако не всегда предварительная преступная деятельность в виде использования ВКП успешно приводит лицо к неправомерному доступу к компьютерной информации. Например, К. используя ВКП DUBrute, осуществлял подбор аутентификационных данных к компьютерным системам. К. неоднократно безуспешно пытался получить доступ к компьютерным

[359] Приговор Советского районного суда г. Казани Республики Татарстан от 11.03.16 г. по делу № 1-35/2016 // ГАС «Правосудие». URL: http://sovetsky.tat.sudrf.ru/ (дата обращения: 13.07.17).

информационным системам: были установлены попытки авторизации, но фактов захода в компьютерную систему не зафиксировано[360].

Иное правило квалификации действует при неправомерном воздействии на КИИ РФ. Так, ч. 2 ст. 274[1] УК РФ регламентирует ответственность за совершения таких действий в качестве единого преступления – *учтенной законодателем совокупности преступлений*. Поэтому при осуществлении неправомерного доступа к охраняемой компьютерной информации, содержащейся в КИИ РФ, с использованием ВКП либо иной компьютерной информации, повлекшее причинение вреда КИИ РФ, квалифицируется только по ч. 2 ст. 274[1] УК РФ. Однако, если такое деяние повлекло только уничтожение, блокирование, модификацию либо копирование компьютерной информации или нейтрализацию средств защиты, без причинения вреда КИИ РФ, такое деяние следует квалифицировать по совокупности преступлений, предусмотренных ч. 1 ст. 274[1] УК РФ и ч. 1 ст. 272 УК РФ.

Таким образом, если приготовление или покушение на какое-то преступление полностью совпадает с другим составом преступления против безопасности компьютерной информации, такие действия квалифицируются по совокупности преступлений, за исключением случая наличия законодательно учтенной совокупности преступлений (ч. 2 ст. 274[1]).

В качестве покушения к преступлению против безопасности компьютерной информации следует квалифицировать деяния субъекта, которому не удалось окончить преступную деятельность по совершению преступления с квалифицированным составом. К примеру, Н. признан виновным в совершении покушения на использование и распространение ВКП (ч. 3 ст. 30, ч. 1 ст. 273 УК РФ), т.е. в умышленных действиях, непосредственно направленных на распространение или использование компьютерных программ, заведомо предназначенных для нейтрализации средств защиты компьютерной информации, если при этом преступление не было доведено до конца по не зависящим от этого

[360] Постановление Советского районного суда г. Казани Республики Татарстан от 11.07.16 г. № 1-416/2016 // ГАС «Правосудие». URL: http://sovetsky.tat.sudrf.ru/ (дата обращения: 13.07.17).

лица обстоятельствам. Судом установлено, что Н. из корыстных побуждений, имея при себе один внешний жесткий диск с записанным на них файлом, заведомо предназначенным для нейтрализации средств защиты компьютерной информации (EmullSmallx32Setup.exe), незаконно установил на один накопитель на жестком магнитном диске программу «1С», после чего собирался установить вредоносную компьютерную программу на компьютер, но свой преступный умысел до конца не довел по не зависящим от него обстоятельствам, а именно потому, что заказчик его торопил и ему не хватило времени[361].

Вопросы возникают также при уяснении правил квалификации рассматриваемых видов преступлений с альтернативными действиями или бездействиями (ст. 273, 274, ч. 1, 3 ст. 274[1] УК), а также с альтернативными последствиями (ст. 272, 273, 274, 274[1] УК). Следует ли квалифицировать действия лица, совершившего одно или несколько действий, альтернативно перечисленных в конструкции составов указанных преступлений, а также действия, которые не смогло довести до конца по независящим от него обстоятельствам по совокупности преступлений? В соответствии с правилами, выработанными в теории квалификации преступлений, такое деяние подлежит квалификации в качестве оконченного преступления и полностью исключает уголовно-правовую оценку как покушение на действие, выполненного частично[362]. Так, Вахитовским районным судом г. Казани Ю. вменено в вину покушение на использование вредоносной компьютерной программы. Материалами дела установлено, что Ю. установил нелицензионные (контрафактные) версии программных обеспечений: Microsoft office 2003 и Windows XP Professional на 4 системных блока ПЭВМ за 2 000 руб., *использовав* при этом файлы WPA_Kill2.1.5, CW.eXe, Windows Loader.exe, после чего Ю. был задержан сотрудниками полиции. Таким образом, Ю. были использованы ВКП для нейтрализации средств защиты компьютерной информации и его действия следует квалифицировать как оконченное преступление.

---

[361] Приговор Вахитовского районного суда г. Казани Республики Татарстан от 08.12.14 г. по делу № 1-450/2014 // ГАС «Правосудие». URL: http://vahitovsky.tat.sudrf.ru/ (дата обращения: 18.07.17).

[362] См.: Корнеева А. В. Указ. соч. С. 62, 65.

Некоторое значение могут иметь вопросы толкования некоторых объективных признаков составов преступлений против безопасности компьютерной информации для квалификации их неоконченными. Так, отдельно необходимо рассмотреть признак получения лицом «*доступа*», наличествующего в ст. 272 УК РФ. Как раскрыто в §2 гл. 2 настоящего исследования, доступ к компьютерной информации может выражаться в получении лицом права на чтение (ознакомление) компьютерной информации, которое не является уголовно-наказуемым последствием.

После ознакомления с компьютерной информацией у лица может возникнуть умысел на осуществление уголовно-наказуемых действий в виде удаления, блокирования, модификации, копирования. Между действием в виде ознакомления и другими действиями может иметься значительный временной промежуток, который также может связываться тем, что лицо не в состоянии получить права на иные виды доступа к компьютерной информации. Поэтому установленный прямой умысел лица на уголовно-наказуемые деяния в виде удаления, блокирования, модификации либо копирования компьютерной информации, непосредственно направленные на такую деятельность, прерванный по независящим от этого лица обстоятельствам, следует квалифицировать как покушение на преступление.

Нами разделяется позиция авторов, согласно которой *доступ* к компьютерной информации *без наступления последствий*, указанных в диспозиции ст. 272 УК РФ, не образует состава преступления, предусмотренного ст. 272 УК РФ[363]. В качестве такого доступа следует рассматривать чтение либо иное ознакомление с компьютерной информацией. За такие действия целесообразно установление административной ответственности.

В свою очередь неправомерное ознакомление с информацией может выступать в качестве приготовления на совершение иных умышленных тяжких либо особо тяжких преступлений: шпионажа, разглашения определенного вида тайны и др.

---

[363] См.: Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. В. М. Лебедев. 14-е изд., перераб. и доп. М.: Юрайт, 2014. С. 804; Преступления в сфере компьютерной информации: квалификация и доказывание. Учебное пособие / Гаврилин Ю.В., Головин Ю. В., Кузнецов А. В., Толстухина Т. В. М.: Книжный мир, 2003. С. 24.

Другие авторы предлагают установить уголовную ответственность за более ранний этап преступной деятельности в отличие от регламентированного. Ими отмечается необходимость изменения конструкции основного состава ст. 272 УК РФ на формальный или формально-материальный и предлагается ввести в него признак визуального ознакомления с информацией[364]. Однако, расширяя таким образом толкование понятия «доступ к компьютерной информации» следует учитывать возможность не только визуального ознакомления с ней, но и способность ее восприятия другими органами чувств. Предположим, что деятелю важно ознакомиться с компьютерной информацией, представленной в виде аудиозаписи. На наш взгляд, такое предложение может выглядеть целесообразным только в части регулирования преступлений, посягающих на критическую информационную инфраструктуру государства.

Неоднозначен вопрос о признании момента окончания *распространения* ВКП в случаях осуществления правоохранительными органами оперативно-розыскных мероприятий (далее – ОРМ) в виде проверочных закупок. Так, Альметьевским городским судом РТ установлено, что Д. незаконно нейтрализовал средство защиты программного продукта «Компас-3D V13» и несанкционированно модифицировал его из демонстрационной версии в версию, использование которой возможно лишь при наличии лицензионного соглашения с правообладателем. После чего Д., не зная о том, что С. оказывает содействие сотрудникам ОЭБ и ПК отдела МВД России по Альметьевскому району и выступает в роли покупателя контрафактной продукции, незаконно сбыл последнему 1 DVD-диск с программным продуктом «Компас-3D V13» с библиотеками[365]. Действия Д. судом были квалифицированы как оконченная преступная деятельность в виде незаконного использования и распространения

---

[364] См. подробнее: Доронин А. М. Уголовная ответственность за неправомерный доступ к компьютерной информации: дис. ... канд. юрид. наук. М., 2003. С. 135; Суслопаров А. В. Указ. соч. С. 132; Малышенко Д. Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации : дис. … канд. юрид. наук. Краснодар, 2008. С. 84; Шарков А. Е. Указ. соч. С. 101.

[365] Приговор Альметьевского городского суда Республики Татарстан от 05 июля 2012 г. по делу № 1-342 // ГАС «Правосудие». URL: http://almetevsky.tat.sudrf.ru/ (дата обращения: 17.07.17).

программы, заведомо приводящей к несанкционированной модификации информации по ч. 1 ст. 273 УК РФ.

Набережночелнинским городским судом РТ квалифицированы действия А. как покушение на распространение ВКП из корыстной заинтересованности (ч. 3 ст. 30 ч. 2 ст. 273 УК РФ), который распространил путем сбыта оптический диск DVD-R, содержащий контрафактную версию программного продукта и вредоносные программы, являющиеся программами генераторами кодов активации программного продукта, заведомо предназначенной для нейтрализации средств защиты программного продукта, оперуполномоченному, действовавшему в рамках ОРМ проверочная закупка, за денежное вознаграждение в размере 300 руб. Квалификация преступления как покушения на преступление судом обоснована тем, что преступные действия А, направленные на незаконный сбыт вышеуказанных программ, не были доведены до конца по независящим от него обстоятельствам, так как вышеуказанный оптический диск был изъят из гражданского оборота[366].

Материалами другого дела установлено, что Р. покушался на распространение компьютерных программ, заведомо предназначенных для нейтрализации средств защиты компьютерной информации, при следующих обстоятельствах. Р. незаконно сбыл (передал) DVD-R диск, содержащий контрафактную версию программного продукта, а также ВКП, являющиеся программами генераторами кодов активации программного продукта, Р.А., действовавшему в рамках ОРМ проверочная закупка, за денежное вознаграждение в размере 700 руб.[367] Действия Р. были квалифицированы по ч. 3 ст. 30 и ч. 2 ст. 273 УК РФ.

По другому делу С. признан виновным в покушении из корыстной заинтересованности на распространение ВКП (ч. 3 ст. 30 и ч. 2 ст. 273 УК РФ). С. скопировал из сети Интернет на диск вредоносные программы. Указанный диск

---

[366] Приговор Набережночелнинского городского суда Республики Татарстан от 31.07.15 г. по делу 1-794 // ГАС «Правосудие». URL: http://naberezhno-chelninsky.tat.sudrf.ru/ (дата обращения: 17.07.17).

[367] Приговор Набережночелнинского городского суда Республики Татарстан от 18.11.14 г. по делу № 1-1134/2014 // ГАС «Правосудие». URL: http://naberezhno-chelninsky.tat.sudrf.ru/ (дата обращения: 17.07.17).

осужденный сбыл за определенную сумму денег в ходе проведения ОРМ проверочная закупка. В апелляционном представлении государственный обвинитель просил изменить и квалифицировать действия С. по ч. 2 ст. 273 УК РФ как оконченное преступление на основании того, что указанный состав преступления является формальным и квалификация по ч. 3 ч.2 ст.30 ст. 273 УК РФ является неверной. Однако суд пришел к выводу, что С. не смог довести до конца действия по распространению программ, заведомо предназначенных для нейтрализации средств защиты компьютерной информации, по не зависящим от него обстоятельствам, поскольку диск с этими программами изъят в ходе проведения ОРМ проверочная закупка[368].

Аналогичная позиция государственного обвинителя наблюдается по делу К. [369] В апелляционном представлении государственный обвинитель просил приговор суда изменить, поскольку совершенное К. преступление по ч. 2 ст. 273 УК РФ не может быть квалифицировано как покушение, с указанием, что оконченным рассматриваемое преступление будет с момента распространения вредоносных программ, создающих угрозу наступления указанных в законе последствий вне зависимости от их наступления. Вместе с тем суд пришел к выводу, что, поскольку действия К., направленные на распространение компьютерных программ, заведомо предназначенных для нейтрализации средств защиты компьютерной информации, до конца не доведены вследствие изъятия диска и имеющиеся на нем программы генераторы кодов фактически не использованы, доводы апелляционного представления не могут быть признаны обоснованными.

Следует отметить, что в судах Самарской области действия по передаче материальных носителей, содержащих вредоносные компьютерные программы, в рамках ОРМ проверочная закупка, которые также изымаются и уничтожаются, т.е. не попадают в дальнейшем в гражданский оборот, судами квалифицируются как

---

[368] Апелляционное определение Верховного Суда Республики Татарстан от 31.05.13 г. по делу № 22-3877 // ГАС «Правосудие». URL: http://vs.tat.sudrf.ru/ (дата обращения 17.07.17).

[369] Апелляционное определение Верховного Суда Республики Татарстан от 31.05.13 г. по делу № 22-3840 // ГАС «Правосудие». URL: http://vs.tat.sudrf.ru/ (дата обращения 17.07.17).

оконченные преступления [370]. Так, в своем апелляционном постановлении Самарский областной суд указал на ошибку в квалификации деяний Ф. судом первой инстанции, переквалифицировав действия Ф. с ч. 1 ст. 273 УК РФ на ч. 3 ст. 30, ч. 1 ст. 273 УК РФ. Доводы вышестоящего суда заключались в следующем. Состав преступления, предусмотренный ч. 1 ст. 273 УК РФ, сконструирован законодателем как формальный. Следовательно, для признания преступления оконченным не требуется реального наступления вредных последствий. То есть сам факт совершения действий по распространению компьютерных программ, заведомо предназначенных для несанкционированной нейтрализации средств защиты компьютерной информации, является оконченным преступлением, независимо от того, удалось ли осуществить их сбыт и причинить реальный ущерб работы ЭВМ. «Поэтому выводы суда первой инстанции о квалификации действий Ф. как покушение на распространение компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированной нейтрализации средств защиты компьютерной информации, ошибочны», – указал Самарский областной суд [371]. Отменив приговор суда первой инстанции, Самарский областной суд направил его на повторное рассмотрение. Впоследствии действия Ф. были квалифицированы как оконченное преступление по ч. 1 ст. 273 УК РФ[372]. Такая аргументация весьма убедительна.

Таким образом, в судебной практике нет выработанной позиции или рекомендации по квалификации преступлений против безопасности компьютерной информации, содержащих в основании доказательственной базы материалы ОРМ в виде проверочной закупки. Проблемы уяснения понятия

---

[370] Приговор Октябрьского районного суда г. Самары Самарской области от 03.02.17 г. по делу № 1-9/2017 // ГАС «Правосудие». URL: http://oktyabrsky.sam.sudrf.ru/ (дата обращения: 13.07.17); Кассационное определение Самарского областного суда от 26.02.13 г. по делу № 22.648/2013 // ГАС «Правосудие». URL: http://oblsud.sam.sudrf.ru/ (дата обращения: 13.07.17); Апелляционное постановление Самарского областного суда по делу № 22-1945/2015 // ГАС «Правосудие». URL: http://oblsud.sam.sudrf.ru/ (дата обращения: 13.07.17); Апелляционное определение Самарского областного суда от 09.12.15 г. по делу № 22-6466/15 // ГАС «Правосудие». URL: http://oblsud.sam.sudrf.ru/ (дата обращения: 13.07.17) и др.

[371] Апелляционное постановление Самарского областного суда от 21.04.14 г. по делу № 22-1673 // ГАС «Правосудие». URL: http://oblsud.sam.sudrf.ru/ (дата обращения: 13.07.17); Приговор Кировского районного суда г. Самары Самарской области по делу № 1-144/2014 // ГАС «Правосудие». URL: http://kirovsky.sam.sudrf.ru/ (дата обращения: 13.07.17).

[372] Приговор Кировского районного суда г. Самары Самарской области от 27.06.14 г. по делу № 1-311/2014 г. // ГАС «Правосудие». URL: http://kirovsky.sam.sudrf.ru/ (дата обращения: 13.07.17).

«распространение» взаимосвязаны также с толкованием другого близкого по содержанию понятия «сбыт», который отсутствует в диспозициях статей главы 28 УК РФ. Высшая судебная инстанция распространение рассматривает, как последствие сбыта. В пункте 13.1 постановления Пленума Верховного Суда РФ от 15.06.2006 г. № 14 «О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами» разъяснил, что изъятие сотрудниками правоохранительных органов из незаконного оборота не влияет на квалификацию преступления как оконченного[373].

На наш взгляд, исходя из доктринального и буквального толкований распространения, его следует рассматривать в качестве синонима сбыта[374]. Поэтому 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 качестве покушения на преступление против безопасности компьютерной информации следует квалифицировать действия лица, направленные на посягательство на *негодный объект*. Под посягательством на негодный объект понимаются действия, не причиняющие вреда охраняемым уголовным законом общественным отношениям, в силу заблуждения лица о свойствах объекта. В качестве примера квалификации преступного посягательства на негодный объект против безопасности компьютерной информации представляется неправомерный

---

[373] диспозиция ст. 238[1] УК РФ не предусматривает в качестве обязательного признака объективной стороны данного преступления наступление последствий в виде незаконного *распространения* (курсив наш – Р. Г.), поэтому их незаконный *сбыт* (курсив наш – Р. Г.) следует считать оконченным преступлением с момента выполнения лицом всех необходимых действий по передаче приобретателю независимо от их фактического получения приобретателем, в том числе, когда данные действия осуществляются в ходе проверочной закупки или иного ОРМ, проводимого в соответствии с Федеральным законом от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности. См.: Рос. газ. 1995. № 160.

[374] См.: Кирьянов Ю.В. Актуальные вопросы рассмотрения уголовных дел, связанных с незаконным оборотом наркотических средств // URL: http://www.oblsud.penza.ru/item/1108/ (дата обращения: 17.07.17); Толковый словарь русского языка под ред. Д.Н. Ушакова. М.: Гос. ин-т Сов. энцикл., 1935-1940. URL: http://dic.academic.ru/dic.nsf/ushakov/1002790 (дата обращения: 17.07.17); Толковый словарь русского языка под ред. С.И. Ожегова и Н.Ю. Шведовой. М., 1997. URL: http://dic.academic.ru/dic.nsf/ogegova/202982 (дата обращения: 17.07.17).

доступ лица к Honeypot (в пер. с англ. – горшочек с медом)[375]. Honeypot – представляет собой систему защиты от несанкционированного доступа к компьютерной информации, так называемую ловушку, полностью имитирующую компьютерную систему с находящейся на ней компьютерной информацией, но фактически не представляющей никакой ценности.

§ 2. Особенности квалификации преступлений против безопасности компьютерной информации, совершенных в соучастии

Статья 32 УК РФ содержит понятие соучастия, согласно которому им признается умышленное совместное участие двух или более лиц в совершении умышленного преступления.

Понятие содержит в себе субъективные и объективные признаки соучастия в преступлении. Субъективными признаками соучастия являются умышленный характер деятельности соучастников, возможность совершения в соучастии только умышленного преступления, взаимная осведомленность каждого из участников. Объективными признаками соучастия являются участие в деятельности двух или более лиц, наличие вклада (физического или интеллектуального) в преступную деятельность каждого из участников (совместность деятельности).

Определение видов и форм совместного участия в преступной деятельности непосредственно связано с квалификацией преступлений. Как справедливо отмечается в литературе, установление вида соучастника способствует установлению его роли в ходе подготовки и совершения конкретного преступления[376]. В качестве видов соучастников в преступлении наряду с исполнителем, в ч. 1 ст. 33 УК РФ законодатель выделяет организатора, пособника и подстрекателя.

---

[375] См.: Honeypot: ловушка для хакера № 1 // Журнал «Хакер», 24.04.2003. URL: https://xakep.ru/2003/04/24/18282/ (дата обращения: 17.07.17).

[376] См.: Уголовное право России. Общая часть: Учебник / Под ред. Ф. Р. Сундурова, И. А. Тарханова. 2-е изд., перераб. и доп. М.: Статут, 2016. С. 395.

Установленные уголовным законом в ст. 33 УК РФ правила квалификации преступлений, совершаемых лицами с распределением ролей, предписывают ссылаться правоприменителю в принимаемом акте не только на пункт, часть и статью Особенной части УК РФ, по которой деяния квалифицируется, но и в зависимости от роли такого лица на соответствующую часть статьи 33 УК РФ. Такая особенность связана с тем, что при сложном соучастии (с распределением ролей) лицо не выполняет объективную сторону преступления. Поэтому исключением из этого правила являются случаи, когда организатор, подстрекатель или пособник является одновременно соисполнителем преступления[377].

Характерные способы совершения преступления в виде форм соучастия находят отражение в ст. 35 УК РФ, которая делит их на совершение преступления группой лиц, группой лиц по предварительному сговору, организованной группой, преступным сообществом (преступной организацией). Выделение форм соучастия в виде организованной группы и преступного сообщества (преступной организации) в науке дискуссионен. С. А. Балеев убедительно доказывает, что соучастие в преступлении в форме преступного сообщества (преступной организации) не является одним из видов форм соучастия по той причине, что целью такого вида совместной преступной деятельности является не совершение единичного преступления, а организованная преступная деятельность[378].

Форму соучастия в виде совершения преступления группой лиц без предварительного сговора законодатель, а также разновидность стечения лиц в одном преступлении в виде организованной группы, законодатель не указывает в качестве квалифицирующих основные составы преступлений против безопасности компьютерной информации.

В судебной практике имеются случаи квалификации действий лиц, совершивших преступления против безопасности компьютерной информации, преступным сообществом (преступной организацией). Как справедливо отмечает С. А. Балеев, возможность совершения преступления преступным сообществом

---

[377] См.: Корнеева А. В. Указ. соч. С. 67.

[378] См.: Балеев С. А. Понятие соучастия в Российском уголовном праве: законодательная регламентация и доктринальное толкование // Учен. зап. Казан. ун-та. Сер. Гуманит. науки. 2009. Т. 151, кн. 4. С. 148.

(преступной организацией) не предусматривается в качестве квалифицирующего ни в одной статье Особенной части УК[379]. Поэтому такие действия находят отражение в квалификации как совокупности компьютерных преступлений со ст. 210 УК РФ с учетом позиции Пленума Верховного Суда РФ, изложенной в постановлении от 10.06.2010 г. № 12 «О судебной практике рассмотрения уголовных дел об организации преступного сообщества (преступной организации) или участии в нем (ней)»[380].

Так, Замоскворецким районным судом г. Москвы действия подсудимых Б., К., Пал., Поп., Г., Ф. квалифицированы по ч. 2 ст. 210 УК РФ (в ред. Федерального закона от 27.12.2009 № 377-ФЗ) как участие в преступном сообществе (преступной организации) в целях совместного совершения тяжких преступлений. Судом было отмечено, что указанное преступное сообщество (преступная организация) характеризуется устойчивостью, сплоченностью, единым умыслом ее участников, длительностью противоправной деятельности, а также отработанной системой совершения преступлений и масштабностью преступной деятельности, затронувшей территорию ряда субъектов Российской Федерации. Кроме этого, данное преступное сообщество (преступная организация) характеризуется знаниями о вредоносном программном обеспечении и его назначении, правилах и порядке его установки и способах модификации, механизма регистрации собственного веб-ресурса и порядка его администрирования, а также использованием полученных навыков работы с вредоносным программным обеспечением в дальнейшей преступной деятельности по хищению денежных средств. Получаемый от этой преступной деятельности доход использовался участниками преступной организации в качестве основного источника существования и обогащения[381].

Повышенная опасность совместного совершения рассматриваемых преступлений при различных групповых формах соучастия отражается также в

---

[379] См.: Балеев С. А. Правовое регулирование ответственности за организацию преступного объединения и участие в нем // Учен. зап. Казан. ун-та. Сер. Гуманит. науки. 2016. Т. 158, кн. 2. С. 592.
[380] Рос. газ. 2010. № 5209 (130).
[381] Приговор Замоскворецкого районного суда г. Москвы от 11.04.16 г. по делу № 1-2/2016 // ГАС «Правосудие». URL: http://zamoskvoretsky.msk.sudrf.ru/ (дата обращения: 18.07.17).

квалифицированных и особо квалифицированных признаках составах этих преступлений. Признаки совершения преступления *группой лиц по предварительному сговору и организованной группой* являются квалифицирующими преступления, ответственность за которые предусмотрена ч. 1 ст. 272, ч. 1 ст. 273 УК РФ, ч.ч. 1-3 ст. 274^1 УК РФ.

Из статистических сведений следует, что доля лиц, совершивших преступления группой лиц, среди лиц, осужденных по гл. 28 УК РФ, в 2013-2016 гг. стабильна и не превышает 6% *(см. Приложение 8)*.

Определение совершения преступления группой лиц по предварительному сговору дается в ч. 2 ст. 35 УК РФ, согласно которому таким преступлением признается, если в нем участвовали лица, заранее договорившиеся о совместном совершении этого преступления. «Заранее» означает предварительную договоренность между лицами о совершении преступления, т.е. до начала выполнения действий неправомерного доступа (ч. 2 ст. 272 УК РФ), создания, распространения или использования ВКП либо иной компьютерной информации подобного рода(ч. 2 ст. 273 УК РФ), неправомерного воздействия на КИИ РФ (ч.1-3 ст. 274^1 УК РФ).

В групповых преступлениях умыслом каждого из соучастников должны охватываться определенные в законе последствия: уничтожение, блокирование, модификация либо копирование компьютерной информации (ч. 2 ст. 272 УК РФ) или возможность причинение вреда КИИ РФ (ч. 2-3 ст. 274^1 УК РФ), либо осознанность или понимание предназначенности, используемых ВКП или иной компьютерной информации подобного рода для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации (ч. 2 ст. 273 УК РФ) или неправомерного воздействия на КИИ РФ (ч. 1 ст. 274^1 УК РФ).

Частью 4 ст. 274^1 УК РФ установлена уголовная ответственность за групповое участие в нарушении правил эксплуатации и правил доступа к объектам КИИ РФ. Однако, как известно, соучастие в преступлении исключается при

неосторожной форме вины, т.е. при совершении неосторожного преступления, коим является деяние, описанное в ч. 3 ст. 274[1] УК РФ.

Как справедливо отмечает А. И. Коробеев, «совершение преступления по предварительному сговору группой лиц следует рассматривать как квалифицированный вид только в тех случаях, когда все соучастники действуют как исполнители»[382]. В том случае, если группа состоит из одного исполнителя и других соучастников, то их деяния не могут квалифицироваться по частям 2 ст.ст. 272 и 273 УК, а также ч. 4 ст. 274[1] УК РФ, предусматривающих признаки совершения преступления группой лиц по предварительному сговору или организованной группой лиц.

По некоторым из рассмотренных нами уголовных дел в правоприменительных актах не дан анализ фактическим данным, подпадающим под признаки соучастия в преступлениях. Так, в материалах дела МВД по РТ ГСУ СЧ по обвинению С. имеются показания обвиняемого, согласно которым неизвестное лицо предложило ему стать его компаньоном в кражах виртуальных денежных средств, рассказало ему возможные способы совершения преступления, установило ему программы, используемые ими совместно для создания фишинговых страниц (комплекса вредоносной компьютерной информации), с помощью которых они незаконно получали регистрационные данные для блокирования доступа к информационным ресурсам[383].

Следует отметить, что при квалификации преступлений установлению всех признаков соучастия препятствует сложность выявления фактических данных о личности соучастников в сети Интернет.

В соответствии с положениями ч. 3 ст. 35 УК РФ неправомерный доступ к охраняемой законом компьютерной информации (ч. 3 ст. 272 УК РФ), а также создание, использование и распространение вредоносных компьютерных программ (ч. 2 ст. 273 УК РФ), неправомерное воздействие на КИИ РФ (ч. 4 ст. 274[1]

---

[382] Полный курс уголовного права: Преступления против общественной безопасности. В 5-ти томах. Т. 4 / Под ред.: А. И. Коробеева. С.-Пб.: Юрид. центр Пресс, 2008. С. 393.

[383] Материалы уголовного дела № 917417 МВД по РТ ГСУ СЧ // Архив Советского районного суда Республики Татарстан.

УК РФ) признаются совершенным организованной группой, если они совершены устойчивой группой лиц, заранее объединившихся для совершения одного или нескольких преступлений.

Как справедливо отмечается в литературе, данному виду совместного участия в преступной деятельности характерны следующие признаки: а) заранее предварительное объединение для совершения преступления; б) высокая степень организованности, включающая: планирование и тщательную подготовку преступной деятельности, распределение ролей между соучастниками; в) устойчивость, т. е. стабильный состав участников, тесная взаимосвязь между ними, согласованность действий участников, постоянство форм и методов преступной деятельности [384] . Например, по одному из дел суд указал, что о наличии квалифицирующего признака совершения преступлений организованной группой свидетельствуют устойчивость, сплоченность, единый умысел ее участников, длительность противоправной деятельности, иерархическое организационное построение, отработанная система совершения преступлений и масштабность преступной деятельности, знания о вредоносном программном обеспечении, его назначении, правил и порядка его установки и способов его модификации, механизма регистрации собственного веб-ресурса и порядка его администрирования, а также использование полученных навыков в дальнейшей преступной деятельности по хищению денежных средств, использование полученного преступного дохода в качестве основного источника существования и обогащения[385].

---

[384] См.: Полный курс уголовного права: Преступления против общественной безопасности. В 5-ти томах. Т. 4 / Под ред.: А.И. Коробеева. С.-Пб.: Юрид. центр Пресс, 2008. С. 393.

[385] Апелляционное определение Московского городского суда от 22.12.16 г. по делу № 10-18451/2016 г. // ГАС «Правосудие». URL: https://www.mos-gorsud.ru/ (дата обращения 18.07.17); Приговор Замоскворецкого районного суда г. Москвы от 11.04.16 г. по делу № 1-2/2016 // ГАС «Правосудие». URL: http://zamoskvoretsky.msk.sudrf.ru/ (дата обращения 18.07.17).

§ 3. Квалификация преступлений против безопасности компьютерной информации при их множественности и способы преодоления конкуренции уголовно-правовых норм

Множественность преступлений выражается в совершении одним лицом нескольких преступлений. Среди видов множественности законодательно регламентируются две ее формы: совокупность преступлений (ч. 1 ст. 17 УК РФ) и рецидив преступлений (ст. 18 УК РФ).

В соответствии с ч. 1 ст. 17 УК РФ совокупностью преступлений признается «совершение лицом двух или более преступлений, ни за одного из которых оно не было осуждено» (реальная совокупность преступлений). Иными словами реальную совокупность преступлений образует совершение лицом нескольких деяний двух или более различных видов преступлений. В таком случае, как известно, каждое из совершенных преступлений квалифицируется по самостоятельной статье (части, пункту) Особенной части УК РФ.

Согласно ч. 2 ст. 17 УК РФ «совокупностью преступлений признается и одно действие (бездействие), содержащее признаки преступлений, предусмотренных двумя или более статьями» УК РФ (идеальная совокупность).

Вторую форму особой преступной деятельности в виде множественности преступлений образует рецидив преступлений (ст. 18 УК РФ). Определение только одного из его видов (специального рецидива) имеет значение только в случаях, специально предусмотренных уголовным законом, – при его учете в качестве квалифицирующего признака. В качестве такого признака среди преступлений против безопасности компьютерной информации он не указывается.

Для разрешения вопросов квалификации по совокупности преступлений против безопасности компьютерной информации (как однородных преступлений), в том числе с иными видами преступлений (в качестве разнородных преступлений), необходимо уделить внимание проблеме определения видового объекта посягательства.

Когда предметом преступлений становятся конфиденциальные сведения, содержащие персональные данные, служебная, коммерческая, банковская тайны и т.д., лицом осуществляется посягательство на такие охраняемые уголовным законом объекты, как право на неприкосновенность частной жизни, личной, семейной, коммерческой, налоговой, банковской, государственной тайн и др. Так, Альметьевским городским судом Республики Татарстан действия Д. были верно квалифицированы по совокупности преступлений, предусмотренных ч. 1 ст. 138 УК РФ и ч. 1 ст. 272 УК РФ, при следующих обстоятельствах. Установлено, что Д. умышленно и тайно, без ведома и согласия потерпевшей, осуществил незаконный доступ к ее анкете на сайте «Вконтакте», изменив логин и пароль, и удалил не менее 600 текстовых сообщений, иные сообщения, фотографические изображения, представляющие тайну для потерпевшей[386].

Вместе с тем на практике при квалификации нередко допускаются ошибки в установлении идеальной совокупности преступлений при посягательстве на несколько объектов. Так, К. и С. в группе лиц по предварительному сговору осуществили неправомерный доступ к файлам базы данных 1С, содержащих сведения о персональных данных пациентов, фактах их обращений за медицинскими услугами, результатах обследований и диагнозах. Указанные файлы принадлежали коммерческой организации, оказывающей медицинские услуги[387]. Очевидно, что врачебная тайна (информация о состоянии здоровья граждан, диагнозах, результатах обследования, самих фактах обращения за медицинской помощью) составляет иной родовой объект уголовно-правовой охраны – личность (раздел 7 УК РФ), а видовой объект уголовно-правовой охраны – конституционное право гражданина на личную тайну (глава 19 УК РФ). Поэтому действия К. и С. образовывают в том числе и состав нарушения неприкосновенности частной жизни.

---

[386] Приговор Альметьевского городского суда Республики Татарстан от 12.11.12 г. по делу № 1-582/2012 // ГАС «Правосудие». URL: http://almetevsky.tat.sudrf.ru/ (дата обращения: 17.07.17).

[387] Постановление Советского районного суда г. Казани Республики Татарстан от 11.07.16 г. № 1-416/2016 // ГАС «Правосудие». URL: http://sovetsky.tat.sudrf.ru/ (дата обращения: 13.07.17).

В правоприменительной практике действия обвиняемых не всегда отражаются в установлении признаков ст. 138 УК РФ как нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Так, по делу № 1-160/2016, рассмотренным Ново-Савиновским районным судом г. Казани, следует, что У. из содержания сообщений на электронном почтовом ящике узнал регистрационные данные, необходимые для доступа к панелям управления доменным именем и хостингом[388]. По другому делу, рассмотренному Ново-Савиновским районным судом г. Казани, установлено, что С. незаконно получал доступ к электронным сообщениям в электронной почте и в социальных сетях других лиц[389]. Следующие материалы уголовного дела показали, что А. и неустановленное лицо скопировали на USB флеш-накопитель личную переписку П.А.В. и П.А.А., хранившуюся на электронных почтовых ящиках, чем нарушили права П.А.В. и П.А.А. на неприкосновенность частной жизни, тайну переписки и почтовых сообщений, предусмотренные ст. 23 Конституции РФ и ст. 9 ФЗ № 149-ФЗ.

Вместе с тем необходимо учитывать, что уголовные дела о преступлениях, ответственность за которые предусмотрена ч. 1 ст. 137 УК РФ и ч. 1 ст. 138 УК РФ, являются делами частно-публичного обвинения, по которым уголовные дела возбуждаются не иначе как по заявлению потерпевшего или его законного представителя. С чем, по всей вероятности, связано отсутствие предъявления обвинений по рассмотренным примерам.

Действия лиц, осуществляющих сбор компьютерной информации, содержащихся на магнитных носителях информации банковских карт (CVV-код, ФИО владельца карты, срок действия карты и др.) с помощью специальных технических средств (т.н. «скиммеров) образуют состав преступления, предусмотренный ст. 138^1 УК РФ «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации», и требуют

---

[388] Приговор Ново-Савиновского районного суда г. Казани Республики Татарстан от 18.05.16 г. по делу № 1-160/2016 // ГАС «Правосудие». URL: http://novo-savinsky.tat.sudrf.ru (дата обращения: 13.07.17).

[389] Материалы уголовного дела № 917417 МВД по РТ ГСУ СЧ // Архив Советского районного суда г. Казани по Республике Татарстан.

соответствующей правовой оценки наряду с квалификацией их с преступлениями против безопасности компьютерной информации. Так, материалами дела установлено, что Г. совершил покушение на незаконный сбыт специальных технических средств, предназначенных для негласного получения информации, при следующих обстоятельствах. Г. передал Б. техническое средство, предназначенное для негласного получения информации, которое находилось в двух коробках, для последующего незаконного сбыта неустановленному лицу в г. М. Далее Б. прибыл на вокзал «Казань-1», передал вышеуказанные коробки проводнику поезда, который согласился передать их неустановленному лицу в М., прибыв в М., по неустановленным причинам не смог передать коробки и добровольно выдал их сотрудникам полиции[390]. Между тем, далее Г. в составе группы лиц по предварительному сговору использовал технические средства для негласного получения компьютерной информации, содержащейся на банковских картах, устанавливая их на банкоматы, и дальнейшего хищения денежных средств. Однако уголовной ответственности за простое использование таких технических средств действующим уголовным законодательством не установлено. В связи с чем, при наличии высокой степени общественной опасности такого деяния наряду с изготовлением и распространением таких средств, считаем необходимым дополнение ст. 138^1 УК РФ признаком «*использования*».

Допускаются ошибки в квалификации действий как идеальной совокупности преступлений, ответственность за которые предусмотрена ст.ст. 146 и 272 УК РФ. Так, органом предварительного расследования взлом компьютерной программы, приведший к возможному ее использованию без лицензионного ключа, охраняемой авторскими правами, квалифицирован как неправомерный доступ к охраняемой законом компьютерной информации, повлекший ее копирование и модификацию. Однако указанные действия не содержали состава преступления, предусмотренного ст. 272 УК РФ, а целиком охватывались

[390] Апелляционное постановление Верховного суда Республики Татарстан от 01.11.16 г. по делу № 22-7630/2016 // ГАС «Правосудие». URL: http://vs.tat.sudrf.ru/ (дата обращения 17.07.17).

составом преступления, предусмотренного ст. 146 УК РФ[391]. По другому делу из обвинения также исключена квалификация по признакам ч. 1 ст. 272 УК РФ как излишне вмененная. Суд постановил, что действия обвиняемого по использованию и распространению контрафактных копий компьютерных программ не могут быть квалифицированы по ч. 1 ст. 272 УК РФ[392].

При изучении материалов судебной практики в некоторых случаях обнаруживается недостаточная квалификация при наличии признаков незаконного получения и разглашения сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ). Так, согласно рапорту об обнаружении признаков преступлений следователем установлено, что К., получив неправомерный доступ к охраняемой законом компьютерной информации, используя вредоносную компьютерную программу, обнаружил, что на компьютерах имеются списки клиентов, которые интересны конкурентам, которые перепродал их, чтобы получить с этого доход. Таким образом, спустя 2 года с момента возбуждения уголовного дела по признакам преступлений, предусмотренных гл. 28 УК РФ, следователем выделено в отдельное производство дело по признакам состава ч. 1 ст. 183 УК РФ. Однако в указанном постановлении следователя не дана предварительная квалификация указанной информации как коммерческой тайны[393].

Без должной квалификации по совокупности со ст. 183 УК РФ остались также действия А., который скопировал персональные данные сотрудников, сведения о налогах, расчетных банковских счетах и движении денежных средств по ним, составляющих налоговую и банковскую тайну[394]. Материалами другого уголовного дела установлено, что у У. на рабочем столе обнаружен файл с названием «На Продажу Картон.txt», содержащий, по предварительной оценке

---

[391] Приговор Кировского районного суда г. Екатеринбурга Свердловской области от 28.12.16 г. по делу № 1-466/2016 г // ГАС «Правосудие». URL: http://kirovsky.svd.sudrf.ru/ (дата обращения: 13.07.17).

[392] Постановление Верх-Исетского районного суда г. Екатеринбурга Свердловской области от 29.09.16 г. по делу № 1-540/2016 // ГАС «Правосудие». URL: http://verhisetsky.svd.sudrf.ru/ (дата обращения: 13.07.17).

[393] Материалы уголовного дела № 350293 СО по расследованию преступлений на территории, обслуживаемой ОП № 15 «Танкодром» СУ Управления МВД России по г. Казани // Архив Советского районного суда г. Казани Республики Татарстан.

[394] Приговор Ново-Савиновского районного суда г.Казани Республики Татарстан от 18.10.16 г. по делу № 1-449/16 // ГАС «Правосудие». URL: http://novo-savinsky.tat.sudrf.ru (дата обращения: 13.07.17).

специалиста, данные платежных пластиковых банковских карт. Однако процессуальных документов, свидетельствующих об обнаружении признаков преступлений, предусмотренных ст. 183 УК РФ, и проверки указанных фактов материалы дела не содержат[395]. По другому делу установлено, что обвиняемые на форумах находили объявления о продаже данных пластиковых карт, приобретали их и впоследствии расплачивались ими на портале государственных и муниципальных услуг[396]. Указанные действия также не нашли отражения при принятии процессуальных решений.

Примером правильной квалификации по совокупности со ст. 183 УК РФ и обоснование такой необходимости дал в одном из своих постановлений Верховный суд Республики Татарстан. Суд не согласился с доводами апелляционных жалоб об излишней квалификации действий Г. по ст. 183 УК РФ в связи с тем, что перечень способов собирания информации диспозицией ст. 183 УК РФ не ограничен. Поскольку Г. собирал сведения, составляющие банковскую тайну, путем неправомерного доступа к компьютерным сетям, его действия правильно квалифицированы по совокупности со ст. 272 УК РФ[397].

Таким образом, родовым объектом уголовно-правовой охраны в рассмотренных случаях, на которую осуществлялось воздействие, является сфера экономики (раздел 8 УК РФ), а видовым – сфера экономической деятельности (гл. 22 УК РФ).

В правоприменительной практике также встречаются случаи квалификации по реальной совокупности преступлений, действий, направленных на посягательство на собственность и сферу экономической деятельности. Нередко путем воздействий тем или иным способом на безопасность компьютерной информации лицам удается похищать денежные средства. В таких случаях

---

[395] Материалы уголовного дела № 83565 МВД по РТ ГСУ СЧ // Архив Советского районного суда г. Казани Республики Татарстан.
[396] Материалы уголовного дела № 314645 МВД по РТ ГСУ СЧ // Архив Советского районного суда г. Казани Республики Татарстан.
[397] Апелляционное постановление Верховного Суда Республики Татарстан по делу № 22-7630 от 01.11.16 г. // ГАС «Правосудие». URL: http://vs.tat.sudrf.ru/ (дата обращения 17.07.17).

действия в зависимости от конкретных обстоятельств, которые мы рассмотрим, будут подлежать квалификации либо по ст. 158 УК РФ, либо по ст. 159^6 УК РФ.

При установлении в таких действиях наличия признаков состава преступления, ответственность за которое предусмотрено ст. 158 УК РФ, следует обратить внимание на следующие обстоятельства. Установлено, что С., неправомерно получив доступ к электронному почтовому ящику, воспользовавшись логином и паролем к «Деньги Mail.Ru», который был «привязан» к электронному почтовому ящику потерпевшего, перечислил денежные средства в общем размере 4 321 руб. 17 коп.[398] Такие действия С. судом были квалифицированы по ст. 158 УК РФ до введения состава компьютерного мошенничества (ст. 159^6 УК РФ).

Следует отличать случаи образования действиями лица реальной совокупности преступлений, ответственность за которые предусмотрена ст.ст. 158 и 272 УК РФ. Такие случаи могут образовываться, когда неправомерный доступ к компьютерной информации является одной из приготовительных стадий для дальнейшего хищения денежных средств без использования компьютерной информации. Так, Верховный суд Республики Татарстан правильно обратил внимание на обстоятельство использования полученной информация в последующем для похищения денежных средств, поэтому действия Г. были правильно квалифицированы по реальной совокупности преступлений, ответственность за которые предусмотрена ст.ст. 158, 272 УК РФ[399]. Так, Г. в составе группы лиц по предварительному сговору путем установки на банкоматы «скиммеров» (технических средств для негласного получения информации) собирал компьютерную информацию, находящуюся на магнитных полосах банковских карт, принадлежащих другим лицам, изготавливал дубликаты таких банковских карт («белый пластик»), на которые записывалась собранная

[398] Материалы уголовного дела № 917417 МВД по РТ ГСУ СЧ // Архив Советского районного суда г. Казани Республики Татарстан.

[399] Апелляционное постановление Верховного Суда Республики Татарстан по делу № 22-7630 от 01.11.16 г. // ГАС «Правосудие». URL: http://vs.tat.sudrf.ru/ (дата обращения: 17.07.17).

информация, являющаяся банковской тайной, и с них денежные средства снимались в банкоматах под видом настоящих[400].

Более того, при квалификации деяний лица по совокупности преступлений, ответственность за которые предусмотрена ст. 158 УК РФ, с преступлениями против безопасности компьютерной информации необходимо обратить внимание на наличие разъяснений, данных Пленумом Верховного Суда РФ от 27.12.2002 г. № 29 «О судебной практике по делам о краже, грабеже и разбое»[401].

Позиции о возможности квалификации одного деяния лица по совокупности преступлений, ответственность за которые предусмотрена ст.ст. 159^6 и 272 УК РФ, весьма различны как в литературе, так и в судебной практике. Так, Самарский областной суд неоднократно в принимаемых постановлениях рассматривал вопрос о возможности квалификации деяния по совокупности преступлений как компьютерное мошенничество и неправомерный доступ к компьютерной информации (ст.ст. 159^6, 272 УК РФ). Например, по одному из дел установлено, что поскольку действия по хищению чужого имущества путем модификации компьютерной информации сопряжены с неправомерным доступом к охраняемой законом компьютерной информации, повлекшим модификацию такой информации, судом правильно квалифицированы действия Х. по совокупности вышеуказанных преступлений. Одно действие подсудимых находит квалификацию по совокупности преступлений и в других рассмотренных делах[402].

Вместе с тем необходимо тщательно устанавливать обстоятельства возможности квалификации указанных преступлений, образующих идеальную совокупность. Так, органами предварительного расследования Г. вменяли

---

[400] Там же.

[401] Бюллетень Верховного Суда РФ. 2003. № 2.

[402] Апелляционное постановление Самарского областного суда от 22.12.14 г. по делу № 22-6029/14 // ГАС «Правосудие». URL: http://oblsud.sam.sudrf.ru/ (дата обращения: 13.07.17); Апелляционное постановление Самарского областного суда от 20.10.14 г. по делу № 22-4759/14 // ГАС «Правосудие». URL: http://oblsud.sam.sudrf.ru/ (дата обращения: 13.07.17); Апелляционное постановление Самарского областного суда от 24.09.14 г. по делу № 22-4263/14 // ГАС «Правосудие». URL: http://oblsud.sam.sudrf.ru/ (дата обращения: 13.07.17); Приговор Автозаводского районного суда города Тольятти Самарской области от 13.04.16 г. по делу № 1-340/2016 // ГАС «Правосудие». URL: http://avtozavodsky.sam.sudrf.ru/ (дата обращения: 13.07.17); Апелляционное определение Московского городского суда от 22.12.2016 г. по делу № 10-18451/16 г. // ГАС «Правосудие». URL: https://www.mos-gorsud.ru/ (дата обращения: 18.07.17) и др.

совокупность рассматриваемых преступлений в связи с тем, что последний через систему дистанционного банковского обслуживания «Сбербанк ОнЛ@йн» осуществлял денежные переводы с личных кабинетов потерпевших на банковскую карту, находящуюся в его распоряжении. Ошибка в квалификации указанных действий по совокупности преступлений состояла в том, что 1) предварительным следствием не установлено причинение вреда охраняемому объекту – нарушению безопасности информации и работы ЭВМ банка; 2) действия подсудимого не повлекли вменяемого последствия в виде модификации – т.к. изменение данных по движению денежных средств по лицевому счету не является модификацией информации, поскольку автоматизированная система «Филиал-Сбербанк» в результате этого не претерпела каких-либо изменений, зафиксировав лишь факт доступа к лицевым счетам и факты перевода денежных средств[403].

Таким образом, при квалификации деяния по признакам составов преступлений, ответственность за которые предусмотрена ст.ст. 159^6 и 272 УК РФ, *следует иметь в виду, что ответственность по данным статьям предусмотрена за совершение различных противоправных действий, с учетом различной объективной стороны преступлений*. При совершении лицом деяния, имеющего все признаки компьютерного мошенничества путем удаления, блокирования, модификации либо копирования компьютерной информации, необходимо установить наличие неправомерного доступа к охраняемой законом компьютерной информации. Если такие признаки установлены (в рамках последствий, наступивших в результате компьютерного мошенничества), то необходима квалификация действия лица как идеальной совокупности преступлений.

В пользу необходимости квалификации совершенного лицом рассматриваемого нами одного деяния по совокупности преступлений свидетельствуют установленная законодателем оценка степени тяжести вреда,

[403] Приговор Промышленного районного суда г. Самары Самарской области от 04.10.16 г. по делу № 1-206/2016 // ГАС «Правосудие». URL: http://promyshleny.sam.sudrf.ru/ (дата обращения: 18.07.17).

причиняемой собственности и сфере компьютерной информации. Как следует из положения ст. 159[6] УК РФ, основным объектом уголовно-правовой охраны является собственность, а дополнительным – компьютерная безопасность. Частью первой рассматриваемой статьи максимальный размер наказания установлен в виде четырех месяцев ареста.

Посягательство на объект в виде компьютерной безопасности, являющийся дополнительным в компьютерном мошенничестве, сопряженным с неправомерным доступом к охраняемой законом компьютерной информации (ч. 1 ст. 272 УК РФ), наказуемо лишением свободы до 2 лет. Однако при осуществлении компьютерного мошенничества санкции необходимо сопоставлять с частью второй ст. 272 УК РФ, а не частью первой, как совершаемое с корыстной заинтересованностью, за которое максимальная санкция установлена в размере до 4 лет лишения свободы.

Таким образом, нельзя ставить знак равенства между компьютерным мошенничеством, совершенным путем удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование компьютерной техники (в т.ч. копирования компьютерной информации), и неправомерным доступом к компьютерной информации (ст. 272 УК РФ). *Поэтому квалификация деяния только по ч. 1 ст. 159[6] УК РФ не отражает в полной мере общественную опасность совершаемого деяния и требует, как уже говорилось, квалификации по совокупности преступлений при наличии соответствующих оснований*. Такое положение полностью отражает актуальность данного разъяснения в п. 12 постановления Пленума Верховного Суда РФ от 27.12.2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате», в котором говорится о необходимости квалификации по совокупности преступлений, ответственность за которые предусмотрена ст.ст. 159 и 272 УК РФ (до дополнения УК РФ ст. 159[6] УК РФ), вопреки имеющимся позициям в литературе[404].

---

[404] Бюллетень Верховного Суда РФ. 2008. № 2.

Квалификацию по реальной совокупности преступлений, ответственность за которые предусмотрена ст.ст. 272 и 165 УК РФ, могут образовывать случаи использования лицами чужих аутентификационных данных, полученных путем обмана или злоупотребления доверием, для дальнейшего безвозмездного доступа в сеть Интернет или безвозмездного пользования любыми другими услугами в сети Интернет. Вместе с тем при квалификации преступлений по признакам состава преступления, предусмотренного ст. 165 УК РФ, следует иметь в виду, что игровая валюта, криптовалюта (Биткоины, Этериумы, Лайткоины, Зекэши, Миткоины и др.) не имеют признаков имущества в гражданско-правовом смысле. Так, СЧ ГСУ МВД по РТ установлено, что подозреваемый С., неправомерно получив доступ к охраняемой законом компьютерной информации, а именно к логину и паролю электронного почтового ящика, получил возможность распоряжаться игровыми денежными средствами Интернет-игры покер. Далее перечислил с игрового аккаунта потерпевшего игровые денежные единицы на свой аккаунт. Таким образом, С. подозревался в совершении преступлений, предусмотренных ч. 1 ст. 272 УК РФ, ч. 1 ст. 165 УК РФ. В ходе расследования уголовного дела следователь прекратил уголовное преследование по признакам ч. 1 ст. 165 УК РФ со следующей формулировкой: условные игровые денежные средства, находящиеся на счете потерпевшего в Интернет-игре покер не подлежали обмену на реальные денежные средства, в сумму условных игровых денежных единиц входили игровые денежные единицы не только приобретенные потерпевшим за свои денежные средства, но и выигранные им условные денежные единицы, а также полученные иным путем, но без проведения за них реальной оплаты денежными средствами[405].

Реальную совокупность преступлений могут образовывать преступления, ответственность за которые предусмотрена ст.ст. 272 и 187 УК РФ. Так, действия К., который удаленно осуществил неправомерный доступ к программному обеспечению коммерческого банка «Кредит», предназначенному для управления

[405] Материалы уголовного дела № 917417 СЧ ГСУ МВД по РТ // Архив Советского районного суда г. Казани Республики Татарстан.

анкетами клиентов и изготовления банковского продукта – расчетных карт «Банк в кармане», используя логины и пароли других сотрудников банка, оформил платежную карту на другое физическое лицо без его ведома, и сбыл неустановленному лицу, квалифицированы по совокупности преступлений как неправомерный доступ к компьютерной информации и неправомерный оборот средств платежей[406].

Не подлежат по общему правилу квалификации преступлений по совокупности деяния альтернативно перечисленные в составах преступлений против безопасности компьютерной информации. Совершение субъектом нескольких деяний, альтернативно перечисленных в диспозиции составов преступлений против безопасности компьютерной информации, образует одно преступление. Так, совокупность преступлений по ч. 2 ст. 272 УК РФ и ч. 2 ст. 273 УК РФ судом усмотрена в следующих действиях: П. совершил модификацию фирменного системного программного обеспечения и нейтрализацию средств защиты игрового устройства, в результате чего произошла нейтрализация механизмов защиты штатного системного программного обеспечения игровой приставки с помощью двухкомпонентного вредоносного программного обеспечения. Он осуществил запись во внутреннюю память игровой приставки частично модифицированного программного обеспечения, позволяющего с использованием метода взлома защиты «переполнение буфера» и с применением вредоносной программы нейтрализовал программные механизмы защиты. В результате своих действий П. из корыстной заинтересованности на игровой приставке обеспечил доступ к запрещенному компанией воспроизведению нелицензионных копий игровых программных продуктов[407]. На наш взгляд, изложенные в фабуле действия П. полностью охватываются признаками ч. 2 ст. 273 УК РФ, а квалификация по ч. 2 ст. 272 УК РФ является излишней.

Тяжкие последствия могут быть причинены любому объекту преступления

---

[406] Приговор Автозаводского районного суда г. Тольятти Самарской области от 13.04.16 г. по делу № 1-340/2016 // ГАС «Правосудие». URL: http://avtozavodsky.sam.sudrf.ru/ (дата обращения: 17.07.17).

[407] Апелляционное определение Самарского областного суда от 25.07.16 г. по делу № 22-4362 // ГАС «Правосудие». URL: http://oblsud.sam.sudrf.ru (дата обращения: 17.07.17).

отличному от охраняемого в гл. 28 УК РФ. В случае наступления *разнородных* последствий деяние может образовывать множественность преступлений, и квалификацию следует производить по правилам совокупности преступлений.

В некоторых случаях преступления против безопасности компьютерной информации отличаются высокой степенью интенсивности воздействия на охраняемые законом объекты. Такая интенсивность объясняется тем, что многие действия компьютерных преступников совершаются с использованием программным средств в автоматическом режиме. Такой характер действий предопределяет вопросы квалификации преступлений по совокупности преступлений в качестве длящегося преступления. Так, Советским районным судом г. Казани установлено, что К. осуществлял компьютерные воздействия в целях нейтрализации средств защиты компьютерной информации из корыстных побуждений следующих информационных систем: 15 мая 2014 г. примерно в период времени с 16 ч. 25 м. по 22 ч. 22 мин. на IP адреса Правительства Астраханской области не менее 23 371 попыток; 26 июня 2014 г. примерно в период времени с 01 часа 26 минут по 02 часа 26 минут на IP-адреса Минсвязи РТ – не менее 117 547 попыток и т.д. Судом такая множественность квалифицирована по ст. 273 УК РФ, как нам представляется, в качестве единичного сложного преступления, состоящего из множества действий[408]. Справедливо, что по данному делу нельзя лицу вменять сотни тысяч действий. Волевой характер действий К. состоял в настройке и запуске одной ВКП, которая осуществляла все перечисленные попытки неправомерного доступа в автоматическом режиме.

Правильная квалификация деяния дана в приговоре Центрального районного суда г. Тольятти действий А. по ч. 3 ст.272, ч. 3 ст. 183, п. «в» ч. 3 ст. 158 УК РФ, совершенного при следующих обстоятельствах. Установлено, что А., являясь оператором отдела голосовой поддержки ЗАО «НКК», действующая на основании заключенного трудового договора (и др. локальных

[408] Приговор Советского районного суда города Казани Республики Татарстан от 17.08.16 г. по делу № 1-416/2016 // ГАС «Правосудие». URL: http://sovetsky.tat.sudrf.ru/ (дата обращения: 13.07.17).

нормативно-правовых актов), т.е., используя свое служебное положение, вошла в компьютерную программу «Электронная система NCCCARD», найдя данные по картам, принадлежащим потерпевшим, не имея заявки банка АКБ «Тольяттихимбанк», в нарушении банковской тайны, незаконно внесла модификацию в компьютерную информацию по вышеуказанным картам, указав в регистрационной карточке зарегистрированный на ее имя номер сотового телефона и другую информацию, которая позволила ей осуществить *несколько переводов* денежных средств на общую сумму в размере 358 000 руб.

По другому делу Д. в период с 19 июня 2012 г. по 20 июня 2012 г. заблокировал доступ потерпевшего к сети Интернет, а затем заблокировал доступ к социальной сети, модифицировав аутентификационные данные. В те же даты, но в другой период времени Д. заблокировал доступ к сети Интернет другого потерпевшего, а затем заблокировал доступ к социальной сети, модифицировав аутентификационные данные. Обвинение по делу было предъявлено по совокупности преступлений, предусмотренных ч. 1 ст. 272 УК РФ. Однако судом вынесен приговор по двум эпизодам преступления, предусмотренного ч. 1 ст. 272 УК РФ в качестве единичного преступления, следовательно, не усматривая в действиях Д. наличия совокупности преступлений. На наш взгляд, судом в приговоре не раскрыта мотивировочная часть, обосновывающая указанную квалификацию[409].

Согласно определению конкуренции (коллизии) уголовно-правовых норм, данному Л. В. Иногамовой-Хегай, под ней понимается «регулирование одного уголовно-правового отношения одновременно двумя или более нормами, приоритетной из которых всегда является одна норма»[410]. *Преодолением* конкуренции называется выбор необходимой уголовно-правовой нормы при квалификации преступлений[411]. В общей теории квалификации преступлений обычно среди видов конкуренции уголовно-правовых норм преступлений

---

[409] Приговор Альметьевского городского суда Республики Татарстан от 12.11.12 г. по делу № 1-582 // ГАС «Правосудие». URL: http://almetevsky.tat.sudrf.ru/ (дата обращения: 17.07.17).

[410] Концептуальные основы конкуренции уголовно-правовых норм: Монография / Л. В. Иногамова-Хегай. М., 2015. С. 11.

[411] Корнеева А. В. Указ. соч. С. 90.

выделяют конкуренция общей и специальной нормы, части и целого. Среди перечисленных видов особую сложность при ее преодолении, на наш взгляд, при квалификации рассматриваемых преступлений вызывает конкуренция общей и специальной нормы. Законодательное правило преодоления конкуренции общей и специальной нормы излагается в ч. 3 ст. 17 УК РФ, согласно которой при их конкуренции квалификация производится по специальной норме.

Рассматриваемый вид конкуренции (общей и специальной нормы) В. Н. Кудрявцев справедливо разделял на конкуренцию норм а) о составах *одного и того же* преступления и б) конкуренцию норм о составах *самостоятельных* преступлений[412]. Конкуренция общей и специальной норм о составах одного и того же преступления по признаку степени общественной опасности в рассматриваемых нами преступлениях может иметь место только между основным и квалифицированным составами (напр., ч. 1 и ч. 2 ст. 272 УК РФ) и между двумя видами квалифицированных составов – специальными нормами (напр., ч. 2 и ч. 3 ст. 272 УК РФ). Конкуренция между основным и привилегированным составами, между двумя видами привилегированных составов и между квалифицированным и привилегированным составов в рассматриваемых нами составах преступлениях не может образовываться.

Правила квалификации в таких случаях следующие. При конкуренции основного и квалифицированного составов преступления против безопасности компьютерной информации квалификация производится по части статьи УК РФ, предусматривающей ответственность за квалифицированное деяние. В случае конкуренции между собой специальных норм квалификация должна производиться по норме, предусматривающей более тяжкий квалифицирующий признак.

С учетом изменений, вступающих в силу в УК РФ с 01 января 2018 г., в главу 28 УК РФ введена по своей сущности норма (ст. 274^{1}), конкурирующая при квалификации преступлений с другими видами преступлений против безопасности компьютерной информации (ст.ст. 272-274), как общие нормы

---

[412] Кудрявцев В. Н. Общая теория квалификации преступлений. М., С. 163.

(ст.ст. 272-274) и специальные нормы (ч. 1-3 ст. 274^1) составов самостоятельных преступлений. При наличии в преступлении всех признаков специальной нормы квалификация преступления должна производиться соответственно по специальной норме, как учитывающая наиболее полно все признаки состава преступления.

Вторым видом конкуренции уголовно-правовых норм является конкуренция части и целого. Как справедливо указывается в литературе, под ней понимаются случаи, когда преступное деяние одновременно подпадает под действие нескольких уголовно-правовых норм: «одна из которых охватывает совершенное деяние в целом, а другая – лишь отдельные его части»[413]. Таким образом соотносятся ч. 1 и ч. 2 ст. 274^1 УК РФ, в которой в ч. 1 использование компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на КИИ РФ, является частью уголовно-правовой нормы, предусмотренной в ч. 2 указанной статьи. Общее правило квалификации преступления регламентирует применять к деянию (при наличии соответствующих признаков) целую норму, т.е. ту, которая наиболее охватывает все фактические обстоятельства содеянного.

[413] Семернева Н. К. Указ. соч. С. 149.

Заключение

Итоговым результатом выполненного исследования являются сформулированные диссертантом основные научные положения, выводы и рекомендации.

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 в данном деле. Это позволяет говорить о квалификации преступления в узком и широком смысле. Понимание квалификации преступления только как содержащуюся в уголовно-процессуальном акте ссылку на пункт, часть и статью УК РФ имеет теоретическое и законодательное основание.

Будучи одной из *форм* (*разновидностей*) уголовно-правовой квалификации квалификация преступления может оказаться одновременно ее следующим *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, 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.

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 которым 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 процесс обеспечения информационной безопасности, одной из целей и результатом которых является «безопасность информации». Таким образом, информационная безопасность представляет собой требуемое состояние объекта, которое достигается посредством урегулированного правом защиты информации. Безопасность информации – это требуемое качество защищенности информации, наличие которого обеспечивает информационная безопасность. Безопасность обращения компьютерной информации – это отсутствие причинения вреда или ее угрозы процессам производства, хранения, использования либо распространения компьютерной информации. Компьютерная безопасность – это состояние защищенности компьютерных и сетевых устройств от угроз различного характера.

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

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.

Основным непосредственным объектом уголовно-правовой охраны и преступления, ответственность за которое предусмотрена ст. 272 УК РФ, следует признавать безопасность охраняемой законом компьютерной информации, которая обеспечивается правомерным доступом к ней, ст. 273 УК РФ – безопасность компьютерной информации и средств защиты компьютерной информации, обеспечиваемая правомерным оборотом компьютерных программ и компьютерной информации, 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, ст. 274^{1} УК РФ – безопасность объектов критической информационной инфраструктуры Российской Федерации.

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.

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. Указанный первый вид вредоносной компьютерной программы либо иной компьютерной компьютерной информации подобного рода является более широким определением по сравнению с ее вторым видом, которая предназначается исключительно для воздействия на критическую информационную инфраструктуру Российской Федерации.

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 времени 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.

Содержание субъективной стороны составов преступлений определяется не только посредством прямого указания на форму вины, но и характеристикой их объективных признаков, поэтому следует признать, 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 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 информации 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).

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.

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.

Кроме основных научных положений, выводов и рекомендаций, выносимых на защиту, диссертантом в работе представлено собственное видение проблемы общей теории квалификации преступлений, сформулированы общие и специальные правила квалификации преступлений против безопасности компьютерной информации с учетом возникающих проблем в правоприменительной практике, а также дана как полная уголовно-правовая характеристика преступлений против безопасности компьютерной информации, так и собственные предложения по толкованию этих норм. В работе выделены новые виды преступлений против безопасности компьютерной информации по непосредственному объекту уголовно-правовой охраны и по характеристике деятельной стороны составов рассматриваемых преступлений. Кроме того, диссертантом проведено деление на виды ВКП на основании их предназначенности на посягательства на ту или иную компьютерную

информацию.

Некоторые из представленных в работе положений и идей являются, как нам представляется, только зачатками новых витков по дальнейшему реформированию законодательства, регулирующего общественные отношения, протекающие в современном информационном обществе.

Например, важно найти решение к универсальному введению в теорию уголовного права определения нематериального предмета преступления; комплексного реформирования уголовного, административного и специального законодательств в сфере информационных технологий в отношении правового регулирования компьютерных систем, построенных на квантовых технологиях, использования блокчейн-технологий и т.д. В таком случае необходимым является проведение междисциплинарных и межотраслевых исследований в сфере информационных технологий для обеспечения соответствующего уровня национальной безопасности.

Представляется перспективным также выделение категории «правонарушения против безопасности компьютерной информации», которая может являться частью «правонарушений в информационной сфере», а правонарушения против безопасности компьютерной информации делить на основании видов правовой ответственности на дисциплинарные проступки, гражданско-правовые деликты, административные правонарушения и уголовные преступления. Поэтому в дальнейшем представляется возможным конструирование новых составов административных правонарушений, направленных на охрану безопасности компьютерной информации, и введение в главу 28 УК РФ конструкций, предусматривающих уголовную ответственность за повторное (либо неоднократное) совершение административных правонарушений, посягающих на безопасность компьютерной информации. Кроме того, введение административной преюдиции в главу 28 УК РФ может послужить «мостиком» между уголовной и административной ответственностями, обеспечивая ступенчатость в наказуемости правонарушений против безопасности компьютерной информации.

На наш взгляд, можно отказаться от раскрытия компьютерно-технических понятий и их уточнения в уголовном законодательстве в целях экономии его содержания, а имеющиеся компьютерно-технические понятия сформулировать в виде бланкетных. Соответствующий понятийный аппарат с учетом предлагаемых нами изменений подлежит раскрыть в специальном законодательстве, например, в ФЗ № 149-ФЗ либо ФЗ № 187-ФЗ в зависимости от объекта уголовно-правовой охраны.

Таким образом, на наш взгляд, указанные направления возможных дальнейших изысканий по данной тематике в достаточной степени ее актуализируют.

Список сокращений и условных обозначений

ВС РФ – Верховный Суд Российской Федерации;

ВКП – вредоносная компьютерная программа;

ГК – Гражданский кодекс Российской Федерации;

КИИ – критическая информационная инфраструктура;

КС РФ – Конституционный Суд Российской Федерации;

МУК СНГ – Модельный уголовный кодекс государств-участников СНГ;

ОРМ – оперативно-розыскные мероприятия;

ОС – операционная система;

ПО – программное обеспечение;

п. – пункт;

пп. – подпункт;

ред. – редакция;

РА – Республика Армения;

РБ – Республика Белоруссия;

РК – Республика Казахстан;

РТ – Республика Татарстан;

РУ – Республика Узбекистан;

РФ – Российская Федерация;

ст.ст. – статьи статей;

СНГ – Содружество Независимых Государств;

т.н. – так называемых;

УК – уголовный кодекс;

УУ ФРГ – Уголовное уложение Федеративной Республики Германия;

указ. соч. – указанные сочинения;

ФЗ – федеральный закон;

ФЗ № 126-ФЗ – Федеральный закон от 07.07.2003 г. № 126-ФЗ «О связи»;

ФЗ № 149-ФЗ – Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

ФЗ № 194-ФЗ – Федеральный закон от 26.07.2017 г. № 194-ФЗ «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"»;

ФЗ № 187-ФЗ – Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

ФЗ № 420-ФЗ – Федеральный закон от 07.12.2011 г. № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации»;

юрид. – юридических.

Список использованной литературы

Законы и иные нормативные правовые акты

1. Конституция Российской Федерации : принята всенародным голосованием 12 дек. 1993 года // Собр. законодательства Рос. Федерации. – 2014 г. – № 31, ст. 4398.

2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 64-ФЗ : принят Гос. Думой Федер. Собр. Рос. Федерации 24 мая 1996 г. : одобр. Советом Федер. Собр. Рос. Федерации 5 июня 1996 г. // Собр. законодательства Рос. Федерации. – 1996. – № 25, ст. 2954.

3. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ : принят Гос. Думой Федер. Собр. Рос. Федерации 22 нояб. 2001 г. : одобр. Советом Федер. Собр. Рос. Федерации 5 дек. 2001 г. : ввод. Федер. законом Рос. Федерации от 18 дек. 2001 г. № 177-ФЗ // Собр. законодательства Рос. Федерации. – 2001. – № 52 (ч. 1), ст. 4921.

4. Гражданский кодекс Российской Федерации (часть четвертая) от 18 дек. 2006 г. № 230-ФЗ : принят Гос. Думой Федер. Собр. Рос. Федерации 24 нояб. 2006 г. : одобр. Советом Федер. Собр. Рос. Федерации 8 дек. 2006 г. : ввод. Федер. законом Рос. Федерации от 18 дек. 2006 г. № 231-ФЗ // Собр. законодательства Рос. Федерации. – 2006. – № 52, ч. 1, ст. 5496.

5. О безопасности : федер. закон Рос. Федерации от 28 декабря 2010 г. № 390-ФЗ : принят Гос. Думой Федер. Собр. Рос. Федерации 7 дек. 2010 г. : одобр. Советом Федерации Федер. Собр. Рос. Федерации 15 дек. 2010 г. // Рос. газ. – 2010. – № 295.

6. О безопасности критической информационной инфраструктуры Российской Федерации : федер. закон Рос. Федерации от 26 июля 2017 г. № 187-ФЗ : принят Гос. Думой Федер. Собр. Рос. Федерации 12 июля 2017 г. : одобр. Советом Федерации Федер. Собр. Рос. Федерации 19 июля 2017 г. // Офиц.

Интернет-портал правовой информации. – 2017. – 26 июля. URL: http://www.pravo.gov.ru (вступает в силу с 1 января 2018 г.).

7. Об информации, информационных технологиях и о защите информации : федер. закон Рос. Федерации от 27 июля 2006 г. № 149-ФЗ : принят Гос. Думой Федер. Собр. Рос. Федерации 08 июля 2006 г. : одобр. Советом Федерации Федер. Собр. Рос. Федерации 14 июля 2006 г. // Собр. законодательства Рос. Федерации. – 2006. – № 31 (1 ч.), ст. 3448.

8. О связи : федер. закон Рос. Федерации от 7 июля 2003 г. № 126-ФЗ : принят Гос. Думой Федер. Собр. Рос. Федерации 18 июня 2003 г. : одобр. Советом Федерации Федер. Собр. Рос. Федерации 25 июня 2003 г. // Рос. газ. – 2003. – № 135.

9. О персональных данных : федер. закон Рос. Федерации от 27 июля 2006 г. № 152-ФЗ : принят Гос. Думой Федер. Собр. Рос. Федерации 8 июля 2006 г. : одобр. Советом Федерации Федер. Собр. Рос. Федерации 14 июля 2006 г. // Рос. газ. – 2006. – № 165.

10. О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации : федер. закон Рос. Федерации от 27 июля 2010 г. № 224-ФЗ : принят Гос. Думой Федер. Собр. Рос. Федерации 2 июля 2010 г. : одобр. Советом Федерации Федер. Собр. Рос. Федерации 14 июля 2010 г. // Рос. газ. – 2010 г. – № 168.

11. О защите детей от информации, причиняющей вред их здоровью и развитию : федер. закон Рос. Федерации от 29 декабря 2010 г. № 436-ФЗ : принят Гос. Думой Федер. Собр. Рос. Федерации 21 декабря 2010 г. : одобр. Советом Федерации Федер. Собр. Рос. Федерации 24 декабря 2010 г. // Собр. законодательства Рос. Федерации. – 2011. – № 1, ст. 48.

12. Об оперативно-розыскной деятельности : федер. закон Рос. Федерации от 12 августа 1995 г. № 144-ФЗ : принят Гос. Думой Федер. Собр. Рос. Федерации 5 июля 1995 г. // Рос. газ. – 1995. – № 160.

13. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы : утв. Указом Президента РФ от 9 мая 2017 г. № 203 // Собр. Законодательства Рос. Федерации. – 2017. - № 20, ст. 2901.

14. Стратегия национальной безопасности Российской Федерации : утв. Указом Президента РФ от 31 декабря 2015 № 683 // Собр. законодательства Рос. Федерации. – 2016. – № 1 (часть II), ст. 212.

15. Доктрина информационной безопасности Российской Федерации : утв. Указом Президента РФ от 5 декабря 2016 г. № 646 // Собр. законодательства Рос. Федерации. – 2016 г. – № 50, ст. 7074.

16. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации : утв. Указом Президента РФ от 3 февраля 2012 г. – № 803 // URL: http://ww.scrf.gov.ru (дата обращения: 17.07.17).

17. Перечень сведений конфиденциального характера : утв. Указом Президента РФ от 6 марта 1997 г. № 188 // Рос. газета. – 1997. – № 51.

18. Правила оказания телематических услуг связи : утв. постановлением Правительства РФ от 10 сентября 2007 г. № 575 // Собр. законодательства Рос. Федерации. – 2007. – № 38, ст. 4552.

19. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» : утв. Приказом Ростехрегулирования от 27 дек. 2006 г. № 373-ст. // М.: Стандартинформ, 2008. – IV, 7, 1 с. – URL: http://consultant.ru (дата обращения: 17.07.17).

20. ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» : утв. Приказом Ростехрегулирования от 18 декабря 2008 г. № 532-ст. // М.: Стандартинформ, 2009. – IV, 15, 1 с. – URL: http://нэб.рф (дата обращения: 18.07.17).

21. ГОСТ Р МЭК 60950-2002 «Безопасность оборудования информационных технологий» : утв. постановлением Госстандарта России от 11

апреля 2002 г. № 148-ст. // М., Стандартинформ, 2005. – XVII, 159, 1 с. – URL: http://consultant.ru/ (дата обращения: 17.07.17).

22. СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы» : утв. постановлением Главного государственного санитарного врача РФ от 13.06.2003 г. № 118 // Зарег. в Министерстве юстиции Российской Федерации 10.06.2013 г. за рег. № 4673.

23. О правовой охране программ для электронных вычислительных машин и баз данных : закон РФ № 3523-I от 23 сент. 1992 г. // (утр. силу).

24. О безопасности : закон РФ от 5 марта 1992 г. № 2446-1 // Рос. газ. – 1992. – № 103. (утр. силу).

Международные правовые акты

25. Конвенция Организации Объединенных Наций Против транснациональной организованной преступности, Палермо, 12 декабря 2000 года : принята резолюцией 55/25 Генеральной Ассамблеи от 15 ноября 2000 года // Собрание законодательства РФ. – 2004. – № 40, ст. 3882.

26. Конвенция Совета Европы О преступности в сфере компьютерной информации, Будапешт, 23 ноября 2001 г. : ETS № 185 // Справочно-правовая система КонсультантПлюс. URL: http://consultant.ru (дата обращения: 17.07.17).

27. Международный пакт о гражданских и политических правах от 16 дек. 1966 г. : принят Резолюцией 2200 (XXI) на 1496-ом пленарном заседании Генеральной Ассамблеи ООН 16 дек. 1966 г. // Ведомости Верховного Совета СССР. – 1976. - № 17, ст. 291. – URL: http://consultant.ru/ (дата обращения: 17.07.17).

28. Модельный Уголовный кодекс государств - участников СНГ: принят постановлением Межпарламентской Ассамблеи государств-участников СНГ от 17 февраля 1996 г. // Справочно-правовая система Гарант. URL: http://garant.ru (дата обращения: 17.07.17).

29. Положение о разработке модельных законодательных актов и рекомендаций Межпарламентской Ассамблеи государств-участников Содружества Независимых Государств : принято в г. Санкт-Петербурге 14.04.2005 г. постановлением 25-8 на 25-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ // Справочно-правовая система КонсультантПлюс. – URL: http://consultant.ru (дата обращения: 17.07.17).

30. Изменения в Модельный Уголовный кодекс для государств – участников Содружества Независимых Государств по вопросам борьбы с преступлениями в информационной сфере : приняты в г. Санкт-Петербург 27 ноября 2015 г. постановлением Межпарламентской Ассамблеей государств-участников СНГ от 27.11.2015 г. № 43-16 // Справочно-правовая система КонсультантПлюс. – URL: http://consultant.ru (дата обращения: 17.07.17).

31. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г., г. Минск // Справочно-правовая система Гарант. URL: http://garant.ru (дата обращения: 17.07.17).

32. Создание глобальной культуры кибербезопасности : принята резолюцией № 58/199 Генеральной Ассамблеей 23 декабря 2003 г. // Резолюции Генеральной Ассамблеи. URL: http://www.un.org/ru/index.html (дата обращения: 17.07.17).

33. Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур : принята резолюцией № 64/2011 Генеральной Ассамблеей 21 декабря 2009 г. // Резолюции Генеральной Ассамблеи. URL: http://www.un.org/ru/index.html (дата обращения: 17.07.17).

Литература

34. Абдеев, Р. Ф. Философия информационной цивилизации. – М.: ВЛАДОС, 1994. – 336 с.

35. Актуальные проблемы информационного права : учебник / Под ред. И. Л. Бачило, М. А. Лапина. – М.: Юстиция, 2016. – 532 с.

36. Балеев С. А. Понятие соучастия в Российском уголовном праве: законодательная регламентация и доктринальное толкование // Учен. зап. Казан. ун-та. Сер. Гуманит. науки. – 2009. – Т. 151, кн. 4. – С. 147-152.

37. Балеев, С. А. Правовое регулирование ответственности за организацию преступного объединения и участие в нем // Учен. зап. Казан. ун-та. Сер. Гуманит. науки. – 2016. – Т. 158, кн. 2. – С. 590-595.

38. Баранова, Е. К. Основы информатики и защиты информации : Учеб. пособие / Е. К. Баранова. – М.: РИОР : ИНФРА-М, 2013. – 183 с.

39. Батурин, Ю. М., Жодзишский, А. М. Компьютерная преступность и компьютерная безопасность. – М.: Юрид. лит., 1991. – 160 с.

40. Батурин, Ю. М., Жодзишский, А. М. Компьютерные правонарушения: криминализация, квалификация, раскрытие // Советское государство и право. – 1990. – № 12. – С. 86-94.

41. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс]: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. – М.: РИОР, 2013. – 222 с.

42. Баштовая, А. Н. Уголовная ответственность и наказание несовершеннолетних // Юрист-Правоведъ. – 2008. – № 3. – С. 36 – 39.

43. Бикмурзин, М. П. Предмет преступления: теоретико-правовой анализ. – М.: Изд-во «Юрлитинформ», 2006. – С. 184.

44. Бражник, С. Д. Актуальные проблемы совершенствования законодательства в сфере компьютерной информации: монография / С.Д. Бражник – Ярославль: МУБиНТ, 2007. – 159 с.

45. Букалерова, Л. А. Уголовно-правовая охрана официального информационного оборота / Под ред. В. С. Комиссарова, Н. И. Пикурова. – М.: Юрлитинформ, 2006. – 360 с.

46. Благов, Е. В. Применение уголовного права (теория и практика). – СПб.: Юридический центр Пресс, 2004. – 505 с.

47. Быков, В. М., Черкасов, В. Н. Новое об уголовной ответственности за создание, использование и распространение вредоносных компьютерных программ // Российский судья. 2012. – № 7. – С. 16-21.

48. Быков, В. М., Черкасов, В. Н. Новый закон о преступлениях в сфере компьютерной информации: ст. 272 УК РФ// Российский судья. 2012. – № 5. – С. 14-19.

49. Венгеров, А. Б. Категория «информация» в понятийном аппарате юридической науки // Советское государство и право. – М.: Наука, 1977. – № 10. – С. 70-78.

50. Вехов, В. Б. Вредоносные компьютерные программы как предмет и средство совершения преступления // Расследование преступлений: проблемы и пути их решения: сб. науч.-практ. тр. – М.: Академия Следственного комитета Российской Федерации, 2015. – № 2. – С. 43-46.

51. Вехов, В. Б. Компьютерные преступления: Способы совершения и раскрытия / Под ред. акад. В. П. Смагоринского – М.: Право и Закон, 1996. – 182 с.

52. Волеводз, А. Г. Противодействие к компьютерным преступлениям: правовые основы международного сотрудничества / А. Г. Волеводз – М.: Юрлитинформ, 2002. – 496 с.

53. Волеводз, А. Г. Российское законодательство об уголовной ответственности за преступления в сфере компьютерной информации // Российский судья. – 2002. – № 9. – С. 34-41.

54. Волеводз, А. Г. Уголовное законодательство об ответственности за компьютерные преступления: опыт разных стран / А. Г. Волеводз, Д. А. Волеводз // Правовые вопросы связи. – 2004. – № 1. – С. 37-48.

55. Волков, Б. С. Мотивы преступлений. – Казань: Изд-во Казанского университета, 1982. – 152 с.

56. Воробьев, В. В. О предмете преступления, его месте в составе преступления и особенностях в компьютерных преступлениях // Символ науки. – 2015. – №. 6. – С. 221-223.

57. Всестороннее исследование проблемы киберпреступности // Управление организации объединенных наций по наркотикам и преступности, проект, февраль, 2013 г. – 360 с. – URL: https://www.unodc.org/documents/organized-crime/cybercrime/ Cybercrime_Study_Russian.pdf (дата обращения: 17.07.17).

58. Гаврилин, Ю. В. Расследование неправомерного доступа к компьютерной информации: Учебное пособие / Под ред. Н. Г. Шурухнова – М.: ЮИ МВД РФ. – Книжный мир, 2001. – 88 с.

59. Галиакберов, Р. Р. Уголовное право. Общая часть. – Краснодар: КубГАУ, 1999. – 259 с.

60. Гаухман, Л. Д. Квалификация преступлений: закон, теория, практика. – 3-е изд., перераб. и дополн. – М.: АО «Центр ЮрИнфоР», 2005. – 457 с.

61. Герцензон А. А. Квалификация преступления. – М.: Изд-во ВЮА КА, 1947. – 26 с.

62. Головненков, П. В. Компьютерная преступность в Германии и система деликтов // Преступления в сфере экономики: российский и европейский опыт: материалы VI совместного российско-германского круглого стола, Москва, 23 октября 2014 г. / ред. кол.: А. И. Рарог, Т. Г. Понятовская. – М.: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2015 – С. 26-35.

63. Головненков, П. В. Уголовное уложение (Уголовный кодекс) Федеративной Республики Германия: научно-практический комментарий и перевод текста закона. – 2-е изд., перераб. и доп. – М.: Проспект, 2014. – 312 с.

64. Гришкин, И. И. Понятие информации. Логико-методологический аспект. – М.: Наука, 1973. – 231 с.

65. Дворецкий, М. Ю. Преступления в сфере компьютерной информации. Научно-практический комментарий к главе 28 Уголовного кодекса Российской Федерации / М.Ю. Дворецкий – Тамбов: Изд-во ТГУ им. Г.Р. Державина, 2005. – 474 с.

66. Дворецкий, М. Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания: Монография. – Тамбов: Изд-во ТГУ им. Г. Р. Державина, 2003. – 197 с.

67. Дроздов, А. В. Человек и общественные отношения – Л.: Изд-во ЛГУ, 1966. – 124 с.

68. Дуюнов, В. К., Хлебушкин, А. Г. Квалификация преступлений: законодательство, теория, судебная практика: Монография. – М.: РИОР: ИНФРА-М, 2012. – 372 с.

69. Дуюнов, В. К., Хлебушкин, А. Г. Квалификация преступлений: законодательство, теория, судебная практика: Монография. – 3-е изд. – М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. – 396 с.

70. Ефремова, М. А. Ответственность за неправомерный доступ к компьютерной информации по действующему законодательству // Вестник Казанского юридического института. 2012. – № 8. – С.54-56.

71. Ефремова, М. А. Уголовно-правовая охрана информации с ограниченным доступом : монограф. / М. А. Ефремова. – Ульяновск. : УлГУ. – 156 с.

72. Ефремова, М. А. Уголовная ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий: монография. – М.: Юрлитинформ, 2015. – 200 с.

73. Защита информации: Учебное пособие / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. – 2-е изд. – М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. – 392 с.

74. Иванцова, Н. В. Модельный Уголовный кодекс для государств участников СНГ и уголовное законодательство Российской Федерации: сравнительно-правовой аспект // Пробелы в российском законодательстве. – 2011. – № 6. – С. 166-169.

75. Информационная безопасность и защита информации: Учебное пособие / Баранова, Е. К., Бабаш, А.В., 3-е изд. – М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. – 322 с.

76. Информационная безопасность : Учебное пособие / Т. Л. Партыка, И. И. Попов. – 5-е изд., перераб. и доп. – М.: Форум : НИЦ ИНФРА-М, 2014. – 432 с.

77. Информационное право : учебник и практикум для академического бакалавриата / И. М. Рассолов. – 4-е изд., перераб. и доп. – М.: Юрайт, 2016. – 346 с.

78. Информационное право: Учебник / Л. Л. Попов, Ю. И. Мигачев, С. В. Тихомиров. – М.: Норма: ИНФРА-М, 2010. – 496 с.

79. Качество уголовного закона: проблемы Особенной части: монография / отв. ред. А. И. Рарог. – М.: Проспект, 2017. – 384 с.

80. Кирьянов, Ю. В. Актуальные вопросы рассмотрения уголовных дел, связанных с незаконным оборотом наркотических средств // Официальный сайт Пензенского областного суда. URL: http://www.oblsud.penza.ru/item/1108/ (дата обращения: 17.07.17).

81. Колмаков, П. А., Воробьев, В. В. К вопросу о содержании и объеме предмета преступлений в сфере компьютерной информации // Вестник ОГУ. – 2011. – №3 (122). – С. 66-69.

82. Кольман, Э. Я. О философских и социальных идеях Норберта Винера // Кибернетика и общество / Отв. ред. А. А. Якушев. – М.: Издательство иностранной литературы, 1958. – 200 с.

83. Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. А. В. Наумов. – М.: Юристъ, 1996. – 824 с.

84. Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. В. М. Лебедев – 14-е изд., перераб. и доп. – М.: Юрайт, 2014. – 1077 с.

85. Комментарий к Уголовному Кодексу Российской Федерации / Под ред. Ю. И. Скуратова, В.М. Лебедева – М.: Норма : ИНФРА-М, 1996. – 592 с.

86. Компьютерная информация под защитой. Правовое и криминалистическое обеспечение безопасности компьютерной информации : монография / А. И. Сотов. – М.: Русайнс, 2015. – 204 с.

87. Концептуальные основы конкуренции уголовно-правовых норм: Монография / Л. В. Иногамова-Хегай – М.: Юр. Норма, НИЦ ИНФРА-М, 2015. – 288 с.

88. Корнеева, А. В. Теоретические основы квалификации преступлений : учеб. Пособие / под. ред. А. И. Рарога. – М. : ТК Велби, Изд-во Проспект, 2007. – 176 с.

89. Корнеева, А. В. Теория и квалификация преступлений: учебное пособие для магистрантов. – М.: Проспект, 2015. – 112 с.

90. Крылов, В. В. Информационные преступления – новый криминалистический объект // Российская юстиция. – 1997. – № 4. – С. 22-23.

91. Крылов, В. В. Расследование преступлений в сфере информации. – М.: Городец, 1998. – 264 с.

92. Кудрявцев, В. Н. Теоретические основы квалификации преступлений // М.: Госюриздат, 1963. – 324 с.

93. Кузнецова, Н. Ф. Проблемы квалификации преступлений : лекции по спецкурсу «Основы квалификации преступлений» / науч. ред. и предисл. академика В. Н. Кудрявцева. – М.: Изд. Дом Городец, 2007. – 336 с.

94. Куринов, Б. А. Научные основы квалификации преступлений. – М.: Изд-во Моск. ун-та, 1984. – 181 с.

95. Курушин, В. Д., Минаев, В. А. Компьютерные преступления и информационная безопасность. – М.: Новый юрист, 1998. – 256 с.

96. Левицкий Г. А. Квалификация преступления (общие вопросы) // Правоведение, Изд-во Ленинг. ун-та. – Ленинград. – 1962. – № 1. – С. 141-145.

97. Литвинов, Д. В. Исследование механизмов противодействия компьютерным преступлениям: организационно-правовые и криминалистические аспекты: монография / Д. В. Литвинов, С. В. Скрыль, А. В. Тямкин. – Воронеж: Изд-во Воронеж. ин-та МВД России, 2009. – 218 с.

98. Лопашенко, Н. А. Посягательства на собственность: монография / Н. А. Лопашенко. – М.: Норма : ИНРФА-М, 2012. – 528 с.

99. Ляпунов, Ю., Максимов, В. Ответственность за компьютерные преступления / Законность. 1997. – № 1. – С. 8-15.

100. Маштаков, И. В. Гражданское правонарушение: определение понятия и юридические признаки // Вестник Самарской гуманитарной академии. Серия: Право, Изд-во: Самарская гуманитарная академия. – Самара. – № 2. – 2007. – С. 29-35

101. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России) // Документ опубликован не был. Доступ из справ.-правовой системы «Консультант Плюс». – URL: http://consultant.ru (дата обращения: 17.07.17).

102. Минбалеев, А. В. К вопросу рассмотрения информации как юридической фикции // Вестник ЮУрГУ. Серия: Право. – 2006. №13 (68). – С. 118-119.

103. Наумов, А. В. Российское уголовное право. Курс лекций. В двух томах. Т.1. Общая часть. – 3-е изд., перераб. и доп. – М.: Юрид. лит., 2004. – 496 с.

104. Наумов, А. В. Российское уголовное право. Курс лекций. В двух томах. Т. 2. Особенная часть. – М.: Юрид. лит., 2004. – 832 с.

105. Наумов, А. В., Новиченко, А. С. Законы логики при квалификации преступлений. – М.: Юридическая литература, 1978. – 104 с.

106. Нестеров, С. В. Общественная безопасность как правовая категория // Аграрное и земельное право. – 2012. – №12 (96). – С. 102-106.

107. Никонов В. А. Основы теории квалификации преступлений (алгоритмический подход): учебное пособие. – Тюмень: Изд-во Тюмен. Ун-та, 2001. – 204 с.

108. Никифоров, Б. С. Объект преступления по советскому уголовному праву. М.: Госюриздат, 1960. – 228 с.

109. Общая теория государства и права. В 3-х т. Т. 2. Право: Академ. курс / М. Н. Марченко, С. Н. Бабурин и др.; Отв. ред. М. Н. Марченко – 4-е изд., перераб. и доп. – М.: Норма : НИЦ ИНФРА-М, 2013. – 816 с.

110. Орловская, Н. А. Зарубежный опыт противодействия компьютерной преступности (проблемы криминализации и наказуемости) // Сборник научных трудов международной конференции «Информационные технологии и безопасность». – Вып. 1. – Киев, 2003. – С. 110–118.

111. Основные положения информационной безопасности: Учебное пособие/ В. Я. Ищейнов, М. В. Мецатунян – М.: Форум, НИЦ ИНФРА-М, 2015. – 208 с.

112. Основы теории информации: Учебное пособие / А. М. Маскаева. – М.: Форум: НИЦ ИНФРА-М, 2014. – 96 с.

113. Пионтковский, А. А. Уголовное право РСФСР, часть Общая. – М., 1924. – 238 с.

114. Полный курс уголовного права: Преступления против общественной безопасности. В 5-ти томах. Т. 4 / Под ред. А. И. Коробеева. – СПб.: Юрид. Центр Пресс, 2008. – 674 с.

115. Практикум по уголовному праву России / Под ред. Ф. Р. Сундурова, М. В. Талан, И. А. Тарханова. – М.: Статут, 2014. – 520 с.

116. Преступления в сфере компьютерной информации: квалификация и доказывание. Учебное пособие // Ю. В. Гаврилин, Ю. В. Головин, А. В. Кузнецов, Т. В. Толстухина / Под ред.: Ю. В. Гаврилина. – М.: Книжный мир, 2003. – 245 с.

117. Причинность и объективная сторона преступления: Монография / З. Б. Соктоев – М.: Юр.Норма, НИЦ ИНФРА-М, 2015. – 256 с.

118. Проблема уголовно-правовой охраны общественных отношений (объект и квалификация преступлений) / В. К. Глистин; Ленинградский ордена Ленина и ордена Трудового Красного Знамени государственный университет им. А. А. Жданова. – Л.: Изд-во ЛГУ, 1979. – 128 с.

119. Проблемы причины и причинной связи в институтах Общей и Особенной частей отечественного уголовного права: вопросы теории, оперативно-следственной и судебной практики / Я. М. Злоченко, И. Я. Козаченко, В. Н. Курченко – С.-Пб.: Юрид. центр Пресс, 2003. – 791 с.

120. Рарог, А. И. Квалификация преступлений по субъективным признакам. – С.-Пб.: Юрид. центр Пресс, 2002. – 304 с.

121. Рарог, А. И. Проблемы квалификации преступлений по субъективным признакам: монография. – М.: Проспект, 2016. – 232 с.

122. Расследование неправомерного доступа к компьютерной информации: Научно-практическое пособие / Под ред. Н. Г. Шурухнова. М.: Щит-М, 1999. – 254 с.

123. Рассолов, М. М. Информационное право: учебное пособие. – М.: Юристъ, 1999. – 400 с.

124. Российское уголовное право. Особенная часть / Под ред. В. Н. Кудрявцева, А. В. Наумова. – М.: Юристъ, 1997. – 496 с.

125. Российское уголовное право. Особенная часть: Учебник / Под ред. А. И. Чучаева. – М.: НИЦ Инфра-М: КОНТРАКТ, 2012. – 448 с.

126. Сабитов, Р. А. Теория и практика квалификации уголовно-правовых деяния: Учеб. пособие. – М.: Изд-во МГУ, 2003. – 144 с.

127. Сабитов, Р. А. Теория и практика уголовно-правовой квалификации: науч.-практич. пособие. – М.: Юрлитинформ., 2013. – 592 с.

128. Саломатина, Е. С. Распространение вредоносных программ для ЭВМ // Юридический вестник Ростовского Государственного экономического университета. – 2007. – № 2. – С.31-35.

129. Семернева, Н. К. Квалификация преступлений (части Общая и Особенная): научно-практическое пособие. – М.: Проспект; Екатеринбург: Издательский дом «Уральская государственная юридическая академия», 2014. – 296 с.

130. Сидоренко, Э. Л. Криптовалюта как новый юридический феномен // Общество и право. 2016. – №3 (57). – С. 193-197.

131. Сизов, А. В. Квалификация нарушений правил эксплуатации ЭВМ, системы ЭВМ или их сети // Информационное право. – 2007. – № 4. – С. 27-30.

132. Сизов, А. В. Неправомерный доступ к компьютерной информации: практика правоприменения // Информационное право. – 2009. – № 1. – С.32-35.

133. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. – М.: Книжный мир, 2009. – 352 с.

134. Соктоев, З. Б. Причинность и объективная сторона преступления: Монография. – М.: НОРМА, ИНФРА-М, 2015. – 256 с.

135. Старичков, М. В. Понятие «компьютерная информация» в российском уголовном праве // Вестник Восточно-Сибирского института Министерства внутренних дел России – Издательство: Восточно-Сибирский институт Министерства внутренних дел Российской Федерации 2014. – С. 16-20.

136. Стратегия национальной безопасности России: теоретико-методологические аспекты: Монография / С. Н. Бабурин, М. И. Дзлиев, А. Д. Урсул. – М.: Магистр: НИЦ Инфра-М, 2012. – 512 с.

137. Сырых, В. М. Теория государства и права: Учебник для вузов. – 3-е изд., перераб. и доп. – М.: ЗАО Юстицинформ, 2007. – 704 с.

138. Таганцев, Н. С. Курс русского уголовного права: Часть общая. Книга 1: Учение о преступлении: [Выпуск 1] / [Сочинение] Н. С. Таганцева, профессора С.-Петербургского университета. – СПб.: Типография М. Стасюлевича, 1874. – VI, 284, VIII с.

139. Тарханов, И. А. О многообразии подходов к определению квалификации преступления и их допустимости // Вестник Волжского университета им. В.Н. Татищева. – Тольятти: ВУиТ, 2012. – Вып. 2 (76). – С. 86-90.

140. Тарханов, И. А. Уголовно-правовая квалификация: понятие и виды // Учен. зап. Казан. ун-та. Сер. Гуманит. науки. – 2009. – Т. 151, кн. 4. – С. 191-198.

141. Тарханов, И. А. Юридическая квалификация: понятие и место в правоприменительном процесс // Российский юридический журнал. – Екатеринбург: Изд-во УрГЮА, 2012. – № 3 (84) – С. 130-140.

142. Толеубекова, Б. Х. Компьютерная преступность: уголовно-правовые и процессуальные аспекты // Караганда, КВШ МВД СССО. – 1991. – 82 с.

143. Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции : монография / А. Ю. Чупрова ; Российская правовая

акад. М-ва юстиции Российской Федерации, Нижегородский гос. ун-т. им. Н. И. Лобачевского. – М.; Нижний Новгород : Изд-во Нижегородского гос. ун-та, 2014. – 560 с.

144. Уголовное право зарубежных стран. Общая и Особенная части : учебник для магистров / под ред. Н. Е. Крыловой. – 4-е изд., перераб. и доп. – М.: Юрайт, 2015. – 1054 с.

145. Уголовное право России. Общая часть: Учебник / Под ред. Ф. Р. Сундурова, И. А. Тарханова. – 2-е изд., перераб. и доп. – М.: Статут, 2016. – 864 с.

146. Уголовное право России. Особенная часть: Учебник / Под ред. Ф. Р. Сундурова, М. В. Талан. – М.: Статут, 2012. – 943 с.

147. Уголовное право России. Части Общая и Особенная. 9-е издание. Учебник / Под ред. А. И. Рарога. – М.: Проспект, 2017. – 928 с.

148. Уголовное право Российской Федерации. Общая и Особенная части: Учебник / Под ред. А. И. Чучаева. – М.: Контракт: ИНФРА-М, 2016. – 704 с.

149. Уголовное право Российской Федерации. Особенная часть: Учебник / Отв. ред. Б. В. Здравомыслов. – М.: Юристъ, 1996. – 559 с.

150. Уголовное право РФ. Особенная часть: Учебник / Л. В. Иногамова-Хегай и др.; Под ред. Л. В. Иногамовой-Хегай. – М.: НИЦ ИНФРА-М, 2013. – 352 с.

151. Уголовное право. Общая часть: Учебник. Издание второе переработанное и дополненное / Под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева. – М.: Контракт : НИЦ ИНФРА-М, 2008. – 560.

152. Уголовное право. Особенная часть: Учебник. Издание второе исправленное и дополненное / под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева. – М.: Юридическая фирма «КОНТРАКТ»: ИНФРА-М, 2008. – 800 с.

153. Уголовное право Российской Федерации. Общая часть: Учебник / Под ред. Л. В. Иногамовой-Хегай. – М.: НИЦ Инфра-М, 2013. – 334 с.

154. Уголовное право. Общая часть: Учебник для вузов / Отв. ред. И. Я. Козаченко. – 5-е изд., перераб. и доп. – М.: Норма: НИЦ ИНФРА-М, 2013. – 592 с.

155. Уголовное право. Особенная часть: Учебник / Отв. ред. И. Я. Козаченко, Г. П. Новоселов. – 5-е изд., изм. и доп. – М.: Норма: НИЦ ИНФРА-М, 2013. – 912 с.

156. Уголовное право. Особенная часть: Учебник / Под ред. Н. И. Ветрова, Ю. И. Ляпунова. – М.: Новый Юрист, КноРус, 1998. – 768 с.

157. Урсул, А. Д. Проблема информации в современной науке. Философские очерки. М.: Наука, 1975. – 286 с.

158. Фаткуллин, Ф. Н. Изменение обвинения. – М.: Юридическая литература, 1971. – 251 с.

159. Хилюта, В. В. Уголовная ответственность за хищения с использованием компьютерной техники // Журнал российского права. – 2014. – № 3 (207). – С. 111-118.

160. Черкасов, В. Н. Изменения законодательства о компьютерных преступлениях. Все ли проблемы решены? // Информационная безопасность регионов. – 2012. – № 2. – С. 116-123.

161. Чупрова, А. Ю. Проблемы квалификации мошенничества с использованием информационных технологий // Уголовное право. – 2015. - № 5. – С. 131-134.

162. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В.Ф. Шаньгин. – М.: ДМК Пресс, 2010. – 544 с.

163. Шершеневич, Г. Ф. Учебник русского гражданского права (по изданию 1907 г.). – М.: Фирма «СПАРК», 1995. – 556 с.

Диссертации и авторефераты

164. Автаева, О. Ю. Гражданские правонарушения : сущность и состав : дис. ... канд. юрид. наук : 12.00.03 / Автаева Ольга Юрьевна. – М., 2004. – 166 с.

165. Айсанов, Р. М. Состав неправомерного доступа к компьютерной информации в российском, международном и зарубежном уголовном законодательстве : дис. ... канд. юрид. наук : 12.00.08 / Айсанов Руслан Мухамедович. – М., 2006. – 191 с.

166. Бегишев, И. Р. Понятие и виды преступлений в сфере обращения цифровой информации: дис. … канд. юрид. наук : 12.00.08 / Бегишев Ильдар Рустамович. – Казань, 2017. – 204 с.

167. Бикмурзин, М. П. Предмет преступления: теоретико-правовой анализ: автореф. дис. … канд. юрид. наук : 12.00.08 / Бикмурзин Максима Павлович. – Саратов, 2005. – 30 с.

168. Букалерова, Л. А. Информационные преступления в сфере государственного и муниципального управления: законотворческие и правоприменительные проблемы : автореф. дис. … д-ра юрид. наук : 12.00.08 / Букалерова Людмила Александровна. – М., 2007. – 65 с.

169. Букалерова, Л. А. Информационные преступления в сфере государственного и муниципального управления: законотворческие и правоприменительные проблемы : дис. … д-ра юрид. наук : 12.00.08 / Букалерова Людмила Александровна. – М., 2007. – 574 с.

170. Воробьев, В. В. Преступления в сфере компьютерной информации: юридическая характеристика составов и квалификация : дис. … канд. юрид. наук : 12.00.08 / Воробьев Виктор Викторович. – Нижний Новгород, 2000. – 201 с.

171. Геллер, А. В. Уголовно-правовые и криминологические аспекты обеспечения защиты электронной информации и Интернета : автореф. дис. … канд. юрид. наук : 12.00.08 / Геллер Артем Владимирович. – М., 2006. – 24 с.

172. Дворецкий, М. Ю. Преступления в сфере компьютерной информации (уголовно-правовое исследование) : дис. ... канд. юрид. наук : 12.00.08 / Дворецкий Михаил Юрьевич. – Волгоград, 2001. – 193 с.

173. Добровольский, Д. В. Актуальные проблемы борьбы с компьютерной преступностью (уголовно-правовые и криминологические проблемы) : дис. ...

канд. юрид. наук : 12.00.08 / Добровольский Дмитрий Владимирович.– М., 2005. – 225 с.

174. Доронин, А. М. Уголовная ответственность за неправомерный доступ к компьютерной информации : дис. ... канд. юрид. наук : 12.00.08 / Доронин Андрей Михайлович. – М., 2003. – 154 с.

175. Жмыхов, А. А. Компьютерная преступность за рубежом и ее предупреждение : дис. … канд. юрид. наук : 12.00.08 / Жмыхов Александр Александрович. – М. 2003. – 178 с.

176. Зинина, У. В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве : дис. ... канд. юрид. наук : 12.00.08 / Зинина Ульяна Викторовна. – М., 2007. – 160 с.

177. Зубова, М. А. Компьютерная информация как объект уголовно-правовой охраны : автореф. дис. … канд. юрид. наук : 12.00.08 / Зубова Марина Александровна. – Казань, 2008. – 27 с.

178. Зубова, М. А. Компьютерная информация как объект уголовно-правовой охраны : дис. … канд. юрид. наук : 12.00.08 / Зубова Марина Александровна. – Казань, 2008. – 215 с.

179. Кабанова, А. Ж. Преступления в сфере компьютерной информации (уголовно-правовые и криминологические аспекты) : автореф. дис. ... канд. юрид. наук : 12.00.08 / Кабанова Анна Жунусовна. – Ростов-на-Дону, 2004. – 28 с.

180. Калмыков, Д. А. Информационная безопасность : Понятие, место в системе уголовного законодательства РФ, проблемы правовой охраны : автореф. дис. … канд. юрид. наук : 12.00.08 / Калмыков Дмитрий Александрович. – Казань, 2005. – 24 с.

181. Калмыков, Д. А. Информационная безопасность: Понятие, место в системе уголовного законодательства РФ, проблемы правовой охраны : дис. … канд. юрид. наук : 12.00.08 / Калмыков Дмитрий Александрович. – Казань, 2005. – 219 с.

182. Карпов, В. С. Уголовная ответственность за преступления в сфере компьютерной информации : дис. ... канд. юрид. наук : 12.00.08 / Карпов Виктор Сергеевич. – Красноярск, 2002. – 202 с.

183. Козаев, Н. Ш. Современные проблемы уголовного права, обусловленные научно-техническим прогрессом : дис. ... д-ра юрид. наук : 12.00.08 / Козаев Нодар Шотаевич. – Краснодар, 2016. – 630 с.

184. Копырюлин, А. Н. Преступления в сфере компьютерной информации: уголовно-правовой и криминологический аспекты : дис. … канд. юрид. наук : 12.00.08 / Копырюлин Алексей Николаевич. – Тамбов, 2007. – 242 с.

185. Красненкова, Е. В. Обеспечение информационной безопасности в Российской Федерации уголовно-правовыми средствами : дис. ... канд. юрид. наук : 12.00.08 / Красненкова Елена Валерьевна. – М., 2006. – 188 с.

186. Крылов, В. В. Основы криминалистической теории расследования преступлений в сфере информации : дис. ... д-ра юрид. наук : 12.00.09 / Крылов Владимир Вадимович. – М., 1998. – 334 с.

187. Кубышкин, А. В. Международно-правовые проблемы обеспечения информационной безопасности государства : автореф. дис. ... канд. юрид. наук : 12.00.10 / Кубышкин Алексей Викторович. – М., 2002. – 32 с.

188. Лопатин, В. Н. Информационная безопасность России : дис. ... д-ра юрид. наук : 12.00.01 / Лопатин Владимир Николаевич. – СПб., 2000. – 433 с.

189. Лопатина, Т. М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности : дис. … д-ра юрид. наук : 12.00.08 / Лопатина Татьяна Михайловна. – М., 2006. – 418 с.

190. Малыковцев, М. М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ : автореф. дис. ... канд. юрид. наук : 12.00.08 / Малыковцев Михаил Михайлович. – М., 2006. – 24 с.

191. Маслакова, Е. А. Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты : дис. ... канд. юрид. наук : 12.00.08 / Маслакова Елена Александровна. – М., 2008. – 198 с.

192. Мнацаканян, А. В. Информационная безопасность в Российской Федерации: уголовно-правовые аспекты : автореф. дис. ... канд. юрид. наук : 12.00.08 / Мнацаканян Аревик Васильевна. – М., 2016. – 41 с.

193. Мнацаканян, А. В. Информационная безопасность в Российской Федерации: уголовно-правовые аспекты : дис. ... канд. юрид. наук : 12.00.08 / Мнацаканян Аревик Васильевна. – М., 2016. – 216 с.

194. Параскевова, С. А. Понятие и социальная сущность гражданского правонарушения: теоретические проблемы : дис. … д-ра юрид. наук : 12.00.03 / Параскевова Светлана Андреевна. – М., 2006. – 367 с.

195. Полушкин, А. В. Информационное правонарушение: понятие и виды : дис. … канд. юрид. наук : 12.00.14 / Полушкин Александр Владимирович. – Екатеринбург, 2009. – 223 с.

196. Полякова, Т. А. Правовое обеспечение информационной безопасности при построении информационного общества в России : автореф. дис. ... д-ра юрид. наук : 12.00.14 / Полякова Татьяна Анатольевна. – М., 2008. – 38 с.

197. Рыбалкин, Н. Н. Природа безопасности : дис. … д-ра филос. наук : 09.00.11 / Рыбалкин Николай Николаевич. – М., 2003. – 407 с.

198. Смирнова, Т. Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации : автореф. ... канд. юрид. наук : 12.00.08 / Смирнова Татьяна Георгиевна. М., 1998. – 28 с.

199. Смирнова, Т. Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации : дис. ... канд. юрид. наук : 12.00.08 / Смирнова Татьяна Георгиевна. – М., 1998. – 161 с.

200. Старичков, М. В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики : автореф. дис. … канд. юрид. наук : 12.00.08 / Старичков Максим Владимирович. – Иркутск, 2006. – 29 с.

201. Степанов-Егиянц, В. Г. Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации :

уголовно-правовой аспект : дис. ... д-ра. юрид. наук : 12.00.08 / Степанов-Егиянц Владимир Георгиевич. – М., 2015. – 389 с.

202. Суслопаров, А. В. Информационные преступления : дис. … канд. юрид. наук : 12.00.08 / Суслопаров Алексей Валерьевич. – Красноярск, 2008. – 249 с.

203. Тропина, Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : дис. ... канд. юрид. наук : 12.00.08 / Тропина Татьяна Львовна. – Владивосток, 2005. – 235 с.

204. Идрисов, Н. Т. Правила квалификации преступлений: понятие, виды, проблема правового регулирования : дис. … канд. юрид. наук. : 12.00.08 / Идрисов Наиль Талгатович. – Самара, 2009. – 193 с.

205. Хисамова, З. И. Уголовно-правовые меры противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий : дис. … канд. юрид. наук : 12.00.08 / Хисамова Зарина Ильдусовна. – Краснодар, 2016. – 222 с.

206. Челноков, В. В. Компьютерная информация как предмет преступления в отечественном уголовном праве : автореф. дис. … канд. юрид. наук : 12.00.08 / Челноков Владислав Валерьевич. – Екатеринбург, 2013. – 31 с.

207. Чупрова, А. Ю. Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции : дис. … док-ра юрид. наук : 12.00.08 / Чупрова Антонина Юрьевна. – М., 2015. – 607 с.

208. Шарков, А. Е. Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации : дис. ... канд. юрид. наук : 12.00.08 / Шарков Александр Евгеньевич. – Ставрополь, 2004. – 174 с.

209. Юрченко, И. А. Информация конфиденциального характера как предмет уголовно-правовой охраны : дис. … канд. юрид. наук : 12.00.08 / Юрченко Ирина Александровна. – М., 2000. – 205 с.

210. Яшков, С. А. Информация как предмет преступления : дис. ... канд. юрид. наук : 12.00.08 / Яшков Сергей Александрович. – Екатеринбург, 2005. – 151 с.

Материалы правоприменительной практики

211. Постановление по делу о проверке конституционности части третьей статьи 138 Уголовного кодекса Российской Федерации в связи с жалобами граждан С. В. Капорина, И. В. Коршуна и других : постановление Конституционного Суда Российской Федерации от 31 марта 2011 г. № 3-П // Рос. газ. – 2011. – №5454 (78).

212. О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности : постановление Пленума Верховного Суда Российской Федерации от 9 фев. 2012 г. № 1 // Бюллетень Верховного Суда РФ. – 2012. – № 4.

213. О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий : постановление Пленума Верховного Суда РФ от 16 окт. 2009 г. № 19 // Рос. газ. – 2009. – № 5031 (207).

214. О практике применения судами законодательства об ответственности за бандитизм : постановление Пленума Верховного Суда РФ от 17 янв. 1997 г. № 1 // Бюллетень Верховного Суда РФ. – 1997. – № 3.

215. О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда РФ от 27 дек. 2007 г. № 51 // Бюллетень Верховного Суда РФ. – 2008. – № 2.

216. О судебной практике по делам о краже, грабеже и разбое : постановление Пленума Верховного Суда РФ от 27 дек. 2002 г. № 29 // Бюллетень Верховного Суда РФ. – 2003. – № 2.

217. О судебной практике рассмотрения уголовных дел об организации преступного сообщества (преступной организации) или участии в нем (ней) : постановление Пленума Верховного Суда РФ от 10 июня 2010 г. № 12 // Рос. газ. – 2010. – № 5209 (130).

218. О применении судами законодательства об ответственности за нарушения в области охраны окружающей среды и природопользования :

постановление Пленума Верховного Суда РФ от 18 окт. 2012 г. № 21 // Рос. газ. – 2012. – № 5924 (251).

219. О судебном приговоре : постановление Пленума Верховного Суда РФ от 29 нояб. 2016 г. № 55 // Рос. газ. – 2016. – № 277.

220. Данные судебной статистики Судебного департамента при ВС РФ // URL: http://www.cdep.ru/index.php?id=79 (дата обращения: 18.07.17).

Источники на иностранных языках

221. Herzog F. Straftaten im Internet, Computerkriminalität und die Cybercrime Convention // Polít. crim. – Vol. 4, № 8 (Diciembre 2009), Doc. 1. – URL: http://www.politicacriminal.cl/Vol_04/n_08/Vol4N8D1.pdf (дата обращения: 17.07.17).

222. Weisser B. Cyber Crime – The information Society and Related Crimes. Section 2 – Special Part. National Report on Germany // electronic Review of the International Association of Penal Law. Preparatory Colloquium Section II. Moscow (Russia), 24-27 April 2013. Criminal Law. Special Part. – URL: http://www.penal.org/sites/default/files/files/RM-8.pdf (дата обращения: 17.07.17).

Законодательство зарубежных стран

223. Уголовное уложение Федеративной Республики Германия от 15 мая 1871 г. // URL: http://www.gesetze-im-internet.de/bundesrecht/stgb/gesamt.pdf (дата обращения: 17.07.17).

224. Уголовный кодекс Грузии от 13 авг. 1999 г. // URL: https://matsne.gov.ge/ka/document/view/16426, https://matsne.gov.ge/ka/document/download/16426/143/ru/pdf (дата обращения: 17.07.17).

225. Уголовный кодекс Республики Армения от 18 апр. 2003 г. // URL: http://www.parliament.am/legislation.php?sel=show&ID=1349&lang=rus (дата обращения: 18.07.17).

226. Уголовный кодекс Республики Беларусь от 9 сент. 1999 г. // URL: http://www.base.spinform.ru/show_doc.fwx?rgn=1977 (дата обращения: 17.07.17).

227. Уголовный кодекс Республики Казахстан от 3 июля 2014 г. №226-V ЗРК // URL: https://online.zakon.kz/Document/?doc_id=31575252#pos=2375;-316 (дата обращения: 18.07.17).

228. Уголовный кодекс Республики Узбекистан от 22 сент. 1994 г. // URL: http://lex.uz/pages/getpage.aspx?lact_id=111457 (дата обращения: 17.07.17).

229. Уголовный кодекс Украины от 5 апр. 2001 г. // СоюзПравоИнформ – URL: http://zakon5.rada.gov.ua/laws/2341-14 (дата обращения: 17.07.17).

230. Уголовный кодекс Франции от 1 янв. 1992 г. // URL: https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719 (дата обращения: 17.07.17).

Приложения

Приложение 1

Проект постановления Пленума Верховного Суда Российской Федерации «О судебной практике по делам о преступлениях против безопасности компьютерной информации»

В целях обеспечения единства практики рассмотрения судами уголовных дел о преступлениях против безопасности компьютерной информации, а также в связи с вопросами, возникающими у судов, Пленум Верховного Суда Российской Федерации, руководствуясь статьей 126 Конституции Российской Федерации и статьями 2 и 5 Федерального конституционного закона от 5 февраля 2014 года № 3-ФКЗ «О Верховном Суде Российской Федерации», постановляет дать следующие разъяснения:

1. При рассмотрении уголовных дел о преступлениях против безопасности компьютерной информации судам необходимо учитывать, что правовое регулирование отношений в сфере обеспечения безопасности компьютерной информации в Российской Федерации осуществляется в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Федеральным законом РФ от 07 июля 2003 г. № 126-ФЗ «О связи», нормативно-правовыми актами, устанавливающими специальные правила к регулированию оборота сведений конфиденциального характера (персональных данных, врачебной, нотариальной, адвокатской тайн, тайны переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.), а также ГОСТ Р 50922-2006 г. «Защита информации. Основные термины и определения», утвержденного Приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст.

2. Обратить внимание судов, что преступления против безопасности компьютерной информации посягают на состояние защищенности компьютерной

информационной сферы, при котором ей не наносится вреда либо отсутствует реальная угроза его нанесения. Под компьютерной информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети Интернет, сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

3. 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 *для* совершения преступления, т.е. с *помощью которых* совершается преступление, в таком случае, они становятся средствами совершения преступления.

4. При квалификации преступлений против безопасности компьютерной информации с учетом признаков объективной стороны составов преступлений против безопасности компьютерной информации необходимо единообразно применять (толковать) термины, используемые в диспозиции уголовно-правовых норм. Соответствующий терминологический аппарат раскрывается в перечисленных в пункте 1 настоящего постановления нормативно-правовых актах, регулирующих отношения в сфере обеспечения безопасности компьютерной информации в Российской Федерации, а также в примечании 1 к статье 272 Уголовного кодекса Российской Федерации (далее – УК РФ).

5. При рассмотрении дел о неправомерном доступе к компьютерной информации следует принимать во внимание, что под неправомерным доступом к компьютерной информации следует понимать получение лицом возможности воздействия на компьютерную информацию в виде чтения, записи или исполнения в компьютерной системе команд, при котором у лица отсутствуют законные права для получения доступа к охраняемой законом компьютерной информации.

6. Обратить внимание судов на то, что при рассмотрении уголовных дел о преступлениях, ответственность за которые предусмотрена статьей 273 и частями 1 и 2 статьи 274^1 УК РФ, под созданием вредоносной компьютерной программы либо иной компьютерной информации, следует понимать рабочий результат деятельности, выразившийся в представлении в объективной форме совокупности данных и команд, который может быть использован для функционирования в информационно-телекоммуникационных сетях, компьютерных устройствах с целью уничтожения, блокирования, модификации, копирования информации, а также с целью нарушения работы информационно-телекоммуникационных сетей.

Под распространением вредоносных программ либо иной компьютерной информации подобного рода следует понимать действия, направленные на получение лицом или передачу таких программ либо компьютерной информации неопределенным кругом лиц.

Под использованием вредоносной компьютерной программы либо иной компьютерной информацией понимается воспроизведение, распространение, копирование и иные действия по ее введению в хозяйственный оборот, в том числе в модифицированной форме.

Если при установлении принадлежности компьютерной программы либо иной компьютерной информации к предметам преступлений, ответственность за которые предусмотрена статьей 273 и частями 1 и 2 статьи 274^1 УК РФ, требуются специальные познания, то суды должны располагать соответствующими заключениями экспертов или специалистов.

7. При рассмотрении дел о преступлениях, предусмотренных статьей 274 и частью 3 статьи 274^1 УК РФ, судам следует указывать в приговоре нарушение каких правил повлекло наступление последствий, указанных в перечисленных статьях, и в чем конкретно выразилось это нарушение.

8. Судам следует принимать во внимание, что под неправомерным воздействием на критическую информационную инфраструктуру Российской Федерации следует понимать действие, имеющие целью повлиять на работу объекта критической информационной инфраструктуры Российской Федерации, в том числе путем уничтожения, блокирования, модификации, копирования, представления или распространения компьютерной информации, содержащейся в ней.

9. При рассмотрении судами уголовных дел о преступлениях против безопасности компьютерной информации под уничтожением компьютерной информации следует понимать ее удаление с средств хранения компьютерной информации вне зависимости от возможности восстановления компьютерной информации.

Под блокированием компьютерной информации следует понимать прекращение или затруднение доступа к информации лиц, имеющих на это право (законных пользователей).

Уголовно-правовую квалификацию неправомерного доступа к охраняемой законом компьютерной информации, повлекший ее блокирование (ст. 272 УК РФ), необходимо осуществлять с учетом реальной общественной опасности такого деяния в зависимости от времени фактического блокирования. Общественно опасными следует признавать такие последствия, которые повлекли существенный вред охраняемым законом правам и интересам. При отсутствии общественной опасности такие деяния следует признавать малозначительными с учетом положения ч. 2 ст. 14 УК РФ.

Под модификацией компьютерной информации понимается любое изменение программного обеспечения, текстовых файлов, изображений, искажающих информацию по сравнению с ее первоначальным состоянием.

Под копированием компьютерной информации понимается точное воспроизведение или запись компьютерной информации с одного носителя компьютерной информации на другой. Под носителями компьютерной информации понимаются материальные объекты, способные длительное время сохранять имеющуюся компьютерную информацию. Например, это магнитные диски (жесткие диски, гибкие диски и др.), оптические диски (CD, DVD и т.д.), переносные накопители данных (флэш-накопители) и др.

Под нейтрализацией средств защиты компьютерной информации (статья 273 УК РФ) следует понимать такое нарушение их функционирования, при котором они прекращают выполнять свои функции.

10. Под несанкционированным уничтожением, блокированием, модификацией, копированием компьютерной информации (статья 273 УК РФ) следует понимать действия, осуществляемые вопреки воле других лиц, которые не могут ими управляться, контролироваться, т.е. в отсутствие их разрешения и уведомления. Для признания деяния преступным важно учитывать отношение правообладателя компьютерной информации с лицом, осуществляющим посягательство на компьютерную информацию. Эти отношения позволяют отличать уголовно-наказуемое деяние от правомерных действий лиц. Такими лицами могут быть специалисты антивирусных компаний или специальных служб, разрабатывающие способы противодействия вредоносным компьютерным программам, выявляющие свойства и признаки компьютерных программ, или работники сервисных служб, обслуживающие компьютерную и периферийную техники.

11. При рассмотрении уголовных дел о преступлениях, ответственность за которые предусмотрена частями 1 и 2 статьи 274^1 УК РФ под неправомерным воздействием на критическую информационную инфраструктуру Российской Федерации следует понимать действие, имеющее целью повлиять на оборот компьютерной информации, в том числе уничтожение, блокирование, модификацию, копирование, представление, распространение компьютерной информации, содержащейся в критической информационной инфраструктуре

Российской Федерации, либо нейтрализации средств защиты указанной информации.

12. При рассмотрении уголовных дел о преступлениях, ответственность за которые предусмотрена частью 2 статьи 274^1 УК РФ, под причинением вреда критической информационной инфраструктуре Российской Федерации следует понимать любой вред, находящийся в прямой причинно-следственной связи с соответствующим неправомерным воздействием.

13. Для правильного вменения в вину предусмотренных уголовным законом последствий в виде уничтожения, модификации и блокирования компьютерной информации необходимо особое внимание уделять установлению прямой причинно-следственной связи между неправомерным доступом к компьютерной информации и наступившими соответствующими последствиями, а также направленности умысла лица.

14. Если неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, повлекший уничтожение, блокирование, модификацию, копирование охраняемой законом компьютерной информации, не привел к причинению вреда, то такое деяние, совершенное с косвенным умыслом либо по легкомыслию, содержащее иные признаки состава преступления, ответственность за которое предусмотрено частью 2 статьи 274^1 УК РФ, следует квалифицировать как неправомерный доступ к компьютерной информации (часть 1 статьи 272 УК РФ) либо по совокупности преступлений, ответственность за которые предусмотрена частью 1 ст. 274^1 УК РФ и частью 1 статьи 272 УК РФ, при наличии соответствующих фактических обстоятельств.

Вместе с тем необходимо обратить внимание на то, что, если лицо желало причинить вред критической информационной инфраструктуре Российской Федерации (часть 2 статьи 274^1 УК РФ), но его действия не привели к указанному вреду по независящим от этого лица обстоятельствам, такие действия подлежат квалификации в качестве покушения на преступление (часть 3 статьи 30, часть 2 статьи 274^1 УК РФ).

15. Субъектом преступлений, ответственность за которые предусмотрена частью 1 статьи 272 и частью 2 статьи 274^1 УК РФ, является физическое, вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста и не обладающее правом доступа к компьютерной информации.

16. Субъектом преступлений, ответственность за которые предусмотрена частью 1 статьи 273 УК РФ и частью 1 статьи 274^1 УК РФ, является физическое, вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста, обладающее совокупностью заранее определенных знаний о предназначенности вредоносной компьютерной программы или компьютерной информации для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации

17. Субъектом преступлений, ответственность за которые предусмотрена статьей 274 и частью 3 статьи 274^1 УК РФ, является физическое, вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста, на которое возлагаются обязанности по соблюдению правил, перечисленных в диспозиции указанных статей УК РФ.

18. Квалификацию преступлений против безопасности компьютерной информации следует осуществлять с учетом того, что субъективная сторона основного состава неправомерного доступа к компьютерной информации (ч. 1 ст. 272 УК РФ) характеризуется любым из видов умысла (как прямым, так и косвенным), а также неосторожностью в виде легкомыслия.

Преступление, ответственность за которое предусмотрено ч. 2 ст. 274^1 УК РФ, с использованием вредоносных компьютерных программ либо иной компьютерной информации подобного рода возможно совершить только умышленно (характерен любой его вид). Неосторожностью в виде легкомыслия может характеризоваться совершение этого преступления 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 информации подобного рода).

Основному составу создания, использования и распространения вредоносных компьютерных программ либо иной компьютерной информации подобного рода (ч. 1 ст. 273), в т.ч. предназначенной для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (ч. 1 ст. 274^1), характерен только прямой умысел.

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).

19. Создание вредоносных компьютерных программ либо иной компьютерной информации является оконченным преступлением с момента появления у лица фактической возможности использования ее вредоносных функций. Поэтому прерывание преступной деятельности лица на одном из этапов (стадий) создания или распространения вредоносной компьютерной программы либо иной компьютерной информации, исключающие возможность их использования, по причинам, не зависящим от виновного лица, должно квалифицироваться как покушение на соответствующее преступление при наличии всех фактических обстоятельств (часть 3 статьи 30, часть 1 статьи 273 УК РФ).

20. Действия обвиняемых, пресеченных в рамках оперативно-розыскного мероприятия проверочная закупка, по использованию (в случае фактического использования) и распространению (в случае передачи сотруднику правоохранительных органов, действующему в рамках соответствующего мероприятия) вредоносной компьютерной программы либо иной компьютерной информации (статья 273 УК РФ) подлежит квалификации в качестве оконченного преступления.

21. Обратить внимание судов, что в качестве покушения на преступление против безопасности компьютерной информации следует квалифицировать действия лица, направленные на посягательство на негодный объект. В качестве негодных объектов могут выступать системы защиты компьютерной информации,

имитирующие компьютерную систему либо компьютерную информацию.

22. Преступления против безопасности компьютерной информации в правоприменительной практике нередко сопряжены с нарушением неприкосновенности частной жизни лица (статья 137 УК РФ), нарушением тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (статья 138 УК РФ), нарушением авторских и смежных прав (статья 146 УК РФ), сбором, хранением, распространением, использованием охраняемой законом компьютерной информации, составляющие коммерческую, налоговую или банковскую тайны (статья 183 УК РФ), незаконным оборотом специальных технических средств, предназначенных для негласного получения информации (статья 138^{1} УК РФ) и другими преступлениями. Такие деяния надлежит квалифицировать по правилам совокупности со ссылкой на соответствующие пункт, часть и статью УК РФ и пункт, часть и статью, предусматривающую ответственность за соответствующее преступление против безопасности компьютерной информации (статьи 272-274^{1} УК РФ).

23. В случаях, когда компьютерное мошенничество (статья 159^{6} УК РФ) сопряжено с неправомерным доступом к компьютерной информации (статья 272 УК РФ) либо с использованием, созданием или распространением вредоносных компьютерных программ (статья 273 УК РФ), содеянное подлежит квалификации по статьей 159^{6} УК РФ, а также, в зависимости от обстоятельств дела, по статьям 272 или 273 УК РФ.

24. Признать утратившим силу абзац 4 пункта 12 постановления Пленума Верховного Суда Российской Федерации от 27 декабря 2007 года № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате».

Приложение 2

Таблица работы с судебными актами

Суд	Номер дела	Дата решения	Информация по делу	Результат слушания
Республика Татарстан				
Советский районный суд г. Казани	1-416/2016	17.08.16	Коровин И.В. – ч.3 ст.272; ч.1 ст.228; ч.2 ст.273 УК РФ; Сибагатов Р.Г. – ч.3 ст.272 УК РФ	Вынесен ПРИГОВОР
Советский районный суд г. Казани	1-219/2016	09.03.16	Усманов Р.М. – ч.1. ст.272 УК РФ	Направлено ПО ПОДСУДНОСТИ (подведомственности)
Советский районный суд г. Казани	1-437/2014	02.07.14	Кондратьев С.В. – ч.1. ст.272 УК РФ	Вынесен ПРИГОВОР
Советский районный суд г. Казани	1-558/2011	27.07.11	Сундуков Р.Р. – п.«в», ч.2 ст.158; ч.1 ст.272 УК РФ	Вынесен ПРИГОВОР
Советский районный суд г. Казани	1-35/2016 (1-731/2015;)	11.03.16	Умаров Р.А. – ч.1. ст.273 УК РФ	Вынесен ПРИГОВОР
Советский районный суд г. Казани	1-517/2015	24.07.15	Глазырин И.Д. – ч.2 ст.159^6 УК РФ;	Вынесен ПРИГОВОР
			Самигуллин Д.И. – ч.2. ст.159^6 УК РФ	
Советский районный суд г. Казани	1-153/2014	22.07.14	Багаутдинов Р.Р. – ч.4 ст.159 УК РФ;	Вынесен ПРИГОВОР
			Портнов Б.А. – ч.4 ст.159 УК РФ	
Приволжский районный суд г. Казани	1-260/2013	27.11.13	Федорова С.Н. – ч.2 ст. 272; ч.1 ст.327 УК РФ	Вынесен ПРИГОВОР
Вахитовский районный суд г. Казани	1-422/2015	18.12.15	Рублев А.А. – ч.3 ст.159^6 УК РФ	Вынесен ПРИГОВОР
Вахитовский районный суд г. Казани	1-450/2014	08.12.14	Нигметзянов И.Г. – ч.2 ст.146; ч.3 ст.30, ч.1 ст.273 УК РФ	Вынесен ПРИГОВОР
Ново-Савиновский районный суд г. Казани	1-449/2016	18.10.16	Алябышев А.Е. – ч.1 ст.272; ч.1 ст.272 УК РФ	Вынесен ПРИГОВОР
Ново-Савиновский районный суд г. Казани	1-160/2016	18.04.16	Усманов Р.М. – ч.1 ст.272 УК РФ	Вынесен ПРИГОВОР
Ново-Савиновский районный суд г. Казани	1-14/2015 (1-448/2014;)	20.05.15	Аббазов Р.Р. – ч.2 ст. 272 УК РФ	Вынесен ПРИГОВОР

Кировский районный суд г.Казани	1-19/2015 (1-381/2014;)	26.01.15	Динерштейн Л.Г. – ч.1 ст.272 УК РФ	Вынесен ПРИГОВОР
Авиастроительный районный суд г. Казани	1-90/2012	17.04.12	Низамов Н.В. – ч.1 ст.272 УК РФ	Вынесен ПРИГОВОР
Московский районный суд г. Казани	1-259/2016	05.09.16	Абанин И.И. – ч.1 ст.273 УК РФ	Вынесен ПРИГОВОР
Альметьевский городской суд	1-137/2013	04.03.13	Мирлачев А.А. – ч.1 ст.272 УК РФ	Вынесен ПРИГОВОР
Альметьевский городской суд	1-582/2012	12.11.12	Давлетшин Р.К. – ч.1 ст.272; ч.1 ст.138; ч.1 ст.138; ч.1 ст.272 УК РФ	Вынесен ПРИГОВОР
Альметьевский городской суд	1-342/2012	05.07.12	Давлеев А.В. – ч.1 ст.273; ч.2 ст.146 УК РФ	Вынесен ПРИГОВОР
Альметьевский городской суд	1-294/2012	24.05.12	Асмакаев А.А. – ч.1 ст.273; ч.2 ст.146 УК РФ	Вынесен ПРИГОВОР
Арский районный суд	1-16/2013	27.03.13	Файзиев М.Р. – ч.1 ст.272 УК РФ	Вынесен ПРИГОВОР
Зеленодольский городской суд	1-218/2013	04.06.13	Постников С.Н. – ч.1 ст.272; ч.2 ст. 272; ч.3 ст.30, ч.1 ст.159^6; ч.3 ст.30, ч.1 ст.159^6; ч.2 ст.273 УК РФ	Вынесен ПРИГОВОР
Зеленодольский городской суд	1-119/2012	24.04.12	Плотников А.А. – ч.2 ст.146; ч.1 ст.273 УК РФ	Вынесен ПРИГОВОР
Зеленодольский городской суд	1-44/2012 (1-571/2011;)	03.04.12	Алексеев И.В. – ч.1 ст.273; ч.2 ст.146 УК РФ	Вынесен ПРИГОВОР
Менделеевский районный суд	1-89/2012	15.10.12	Сафин И.М. – ч.2 ст. 272 УК РФ	Уголовное дело ПРЕКРАЩЕНО за примирением сторон
Набережночелнинский городской суд	1-1467/2016	05.12.16	Дудковский Е.М. – ч.2 ст.146; ч.2 ст.273 УК РФ	Вынесен ПРИГОВОР
Набережночелнинский городской суд	1-794/2015	31.07.15	Артемов А.В. – ч.3 ст.30, ч.2 ст.146; ч.3 ст.30, ч.2 ст.273 УК РФ	Вынесен ПРИГОВОР
Набережночелнинский городской суд	1-789/2015	31.07.15	Филимонов М.В. – ч.3 ст.30, ч.2 ст.146; ч.3 ст.30, ч.2 ст.273 УК РФ	Вынесен ПРИГОВОР
Набережночелнинский городской суд	1-154/2015	10.02.15	Юминов В.Р. – ч.3 ст.30, ч.2 ст.146; ч.3 ст.30, ч.2 ст.273 УК РФ	Вынесен ПРИГОВОР
Набережночелнинский городской суд	1-1134/2014	18.11.14	Рязанов Е.А. – ч.3 ст.30, ч.2 ст.146; ч.3 ст.30, ч.2 ст.273 УК РФ	Вынесен ПРИГОВОР
Набережночелнинский городской суд	1-830/2014	08.08.14	Ахунов А.М. – ч.3 ст.30, ч.2 ст.146; ч.3 ст.30, ч.2 ст.273 УК РФ	Вынесен ПРИГОВОР
Набережночелнинский городской суд	1-620/2014	11.06.14	Мухаметшин А.Р. – ч.3 ст.30, ч.2 ст.146; ч.3 ст.30, ч.2 ст.273 УК РФ	Вынесен ПРИГОВОР
Набережночелнинский городской суд	1-1035/2013	06.09.13	Кузьминых А.А. – ч.3 ст.30, ч.2 ст.146, ч.3 ст.30, ч.2 ст.273	Вынесен ПРИГОВОР

Набережночелнинский городской суд	1-862/2013	26.07.13	Ахмаджанов А.Т. – ч.3 ст.30, ч.2 ст.146, ч.3 ст.30, ч.2 ст.273	Вынесен ПРИГОВОР
Набережночелнинский городской суд	1-184/2013	11.04.13	Кривенко К. М. – ч.2 ст.146, ч.2 ст.273	Вынесен ПРИГОВОР
Набережночелнинский городской суд	1-183/2013	11.04.13	Савтырук И.Н. – ч.2 ст.146, ч.2 ст.273	Вынесен ПРИГОВОР
Тукаевский районный суд	1-22/2015	12.02.15	Садретдинов Р.Р. – ч.2 ст.146; ч.2 ст.273 УК РФ	Вынесен ПРИГОВОР
Чистопольский городской суд	1-80/2012	04.05.12	Валиев Д.И. – ч.1 ст.272; ч.1 ст.272; ч.1 ст.272; ч.1 ст.272 УК РФ	Вынесен ПРИГОВОР
Верховный суд Республики Татарстан	22-8753/2016	13.12.16	Алябышев А.Е. – УК РФ: ч.1 ст.272	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Верховный суд Республики Татарстан	22-7630/2016	01.11.2016	Галиев Р.Ф. – УК РФ: ч.2 ст. 69; ч.3 ст.30 – п.«а» ч.2 ст. 158; ч.3 ст.183; ч.3 ст.30 – ч.3 ст.183; ч.3 ст.30 – ч.3 ст.272	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Верховный суд Республики Татарстан	22К-4609/2016	10.06.2016	Коровин И.В. – УК РФ: ст. 228 ч.1; ч.3 ст.272; ч.2 ст.273	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Верховный суд Республики Татарстан	22-4290/2016	28.06.2016	Усманов Р.М. – УК РФ: ч.1 ст.272	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Владимирская область				
Вязниковский городской суд	1-301/2011	11.10.2011	Юсов В.С. – ч.1 ст.273 УК РФ	Вынесен ПРИГОВОР
Владимирский областной суд	22-1372/2015	16.06.2015	Ловушкин А.Г. - УК РФ: ч.1 ст.272; ч.1 ст.273	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ
Владимирский областной суд	22-2391/2015	27.10.2015	Розов В.Н. - УК РФ: ч.2 ст.146; ч.1 ст.273	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Владимирский областной суд	22-1372/2015	16.06.2015	Ловушкин А.Г. - УК РФ: ч.1 ст.272; ч.1 ст.273	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Фрунзенский районный суд г. Владимира	1-107/2013	11.04.2013	Скидан Д.А. - ч.2 ст.273; ч.1 ст.272; ч.1 ст.272; ч.1 ст.272; ч.1 ст.272; ч.2 ст. 272; ч.1 ст.273; ч.1 ст.273; ч.1 ст.273; ч.1 ст.273 УК РФ	Вынесен ПРИГОВОР
Фрунзенский районный суд г. Владимира	1-84/2017	21.06.17	Антонов А.А. - ч.2 ст.146; ч.1 ст.273 УК РФ	Уголовное дело ПРЕКРАЩЕНО
Фрунзенский районный суд г. Владимира	1-49/2016	02.03.16	Пекарский А.С. - ч.2 ст.146; ч.2 ст.273 УК РФ	Уголовное дело ПРЕКРАЩЕНО
Фрунзенский районный суд г. Владимира	1-107/2013	11.04.13	Скидан Д.А. - ч.2 ст.273; ч.1 ст.272; ч.1 ст.272; ч.1 ст.272; ч.1 ст.272; ч.2 ст. 272; ч.1 ст.273; ч.1 ст.273; ч.1 ст.273; ч.1 ст.273 УК РФ	Вынесен ПРИГОВОР
Фрунзенский районный суд г. Владимира	1-47/2013	23.01.13	Вьюнов Д.В. - ч.2 ст.146; ч.2 ст.273 УК РФ	Уголовное дело ПРЕКРАЩЕНО

Фрунзенский районный суд г. Владимира	1-23/2012 (1-324/2011;)	15.05.12	Растяженко А.В. - п.”в” ч.3 ст.146; ч.1 ст.273 УК РФ	Уголовное дело ПРЕКРАЩЕНО
Фрунзенский районный суд г. Владимира	1-205/2010	06.07.10	Мошкин А.В. - ч.1 ст.273; ч.1 ст.146УК РФ	Вынесен ПРИГОВОР
Октябрьский районный суд г. Владимира	1-217/2016	26.05.2016	Маров А.А. - ч.2 ст.146; ч.1 ст.273 УК РФ	Уголовное дело ПРЕКРАЩЕНО
Октябрьский районный суд г. Владимира	1-135/2016	07.04.2016	Хитев С.А. - ч.1 ст.273; ч.2 ст.146 УК РФ	Уголовное дело ПРЕКРАЩЕНО
Октябрьский районный суд г. Владимира	1-106/2016	02.03.2016	Махота А.А. - ч.2 ст.146; ч.1 ст.273 УК РФ	Уголовное дело ПРЕКРАЩЕНО
Октябрьский районный суд г. Владимира	1-456/2015	11.12.2015	Горелов К.О. - ч.2 ст.273 УК РФ	Вынесен ПРИГОВОР
Октябрьский районный суд г. Владимира	1-422/2015	10.12.2015	Фомин Ю.С. - ч.2 ст.146; ч.2 ст.273; ч.2 ст.273 УК РФ	Уголовное дело ПРЕКРАЩЕНО
Октябрьский районный суд г. Владимира	1-312/2015	11.08.2015	Русаков Р.Н. - ч.1 ст.273; ч.2 ст.146 УК РФ	Вынесен ПРИГОВОР
Октябрьский районный суд г. Владимира	1-270/2015	07.07.2015	Куркин А.С. - ч.1 ст.273; ч.1 ст.273; ч.2 ст.146 УК РФ	Вынесен ПРИГОВОР
Октябрьский районный суд г. Владимира	1-268/2015	15.07.2015	Сущинин А.А. - ч.2 ст.146; ч.1 ст.273; ч.1 ст.273; ч.2 ст.146 УК РФ	Вынесен ПРИГОВОР
Октябрьский районный суд г. Владимира	1-224/2015	11.06.2015	Олейник А.В. - ч.2 ст.146; ч.1 ст.273 УК РФ	Уголовное дело ПРЕКРАЩЕНО
Октябрьский районный суд г. Владимира	1-220/2015	26.05.2015	Горшунов А.А. - ч.2 ст.146; ч.1 ст.273 УК РФ	Уголовное дело ПРЕКРАЩЕНО
Октябрьский районный суд г. Владимира	1-207/2015	15.06.2015	Гущин А.А. - ч.2 ст.146; ч.1 ст.273 УК РФ	Уголовное дело ПРЕКРАЩЕНО
Октябрьский районный суд г. Владимира	1-128/2015	02.04.2015	Семенов Д.Н. - ч.1 ст.273; ч.2 ст.146 УК РФ	Уголовное дело ПРЕКРАЩЕНО
Октябрьский районный суд г. Владимира	1-62/2015 (1-490/2014;)	11.02.2015	Тихомиров А.Н. - ч.2 ст.146; ч.1 ст.273; ч.1 ст.273; ч.2 ст.146 УК РФ	Уголовное дело ПРЕКРАЩЕНО
Октябрьский районный суд г. Владимира	1-61/2015 (1-489/2014;)	24.03.2015	Шарифов Р.Д. - ч.1 ст.273; ч.2 ст.146 УК РФ	Уголовное дело ПРЕКРАЩЕНО
Октябрьский районный суд г. Владимира	1-438/2014	23.12.2014	Карсаков В.В. - ч.2 ст.146; ч.1 ст.273; ч.2 ст.146 УК РФ	Уголовное дело ПРЕКРАЩЕНО
Октябрьский районный суд г. Владимира	1-314/2014	05.11.2014	Анисимов И.В. - ч.2 ст.146; ч.1 ст.273; ч.1 ст.273; ч.1 ст.273; ч.1 ст.273; ч.1 ст.273; ч.1 ст.30, ч.2 ст.146 УК РФ	Уголовное дело ПРЕКРАЩЕНО
Октябрьский районный суд г. Владимира	1-313/2014	25.08.2014	Пучков М.А. - ч.1 ст.273; ч.2 ст.146 УК РФ	Уголовное дело ПРЕКРАЩЕНО
Октябрьский районный суд г. Владимира	1-221/2014	11.06.2014	Шаршин И.В. - ч.2 ст.146; ч.1 ст.273; ч.2 ст.273; ч.2 ст.273; ч.2 ст.273; ч.2 ст.273 УК РФ	Уголовное дело ПРЕКРАЩЕНО
Октябрьский районный суд г. Владимира	1-16/2014 (1-400/2013;)	18.06.2014	Мошкаров Д.А. - ч.2 ст.273; ч.2 ст.273; ч.2 ст.146 УК РФ	Вынесен ПРИГОВОР
Октябрьский районный суд г. Владимира	1-262/2013	27.06.2013	Бабников В.А. - ч.2 ст.146; ч.1 ст.273 УК РФ	Вынесен ПРИГОВОР
Октябрьский районный суд г. Владимира	1-223/2013	22.05.2013	Самарин Н.Ю. - ч.1 ст.273; ч.2 ст.146 УК РФ	Вынесен ПРИГОВОР
Октябрьский районный суд г. Владимира	1-208/2013	03.06.2013	Санков В.Н. - ч.2 ст.146; ч.1 ст.273; ч.1 ст.273; ч.1 ст.273; ч.1	Уголовное дело ПРЕКРАЩЕНО

			ст.273 УК РФ	
Октябрьский районный суд г. Владимира	1-78/2013 (1-510/2012;)	31.05.2013	Рассказчиков Д.Н. - ч.1 ст.273; п.”в” ч.3 ст.146 УК РФ	Вынесен ПРИГОВОР
Октябрьский районный суд г. Владимира	1-364/2012	23.10.2012	Тупицын А.В. - ч.2 ст.146; ч.1 ст.273 УК РФ	Уголовное дело ПРЕКРАЩЕНО
Октябрьский районный суд г. Владимира	1-338/2012	31.07.2012	Тихомиров А.Н. - ч.2 ст.146; ч.1 ст.273 УК РФ	Вынесен ПРИГОВОР
Октябрьский районный суд г. Владимира	1-337/2012	28.09.2012	Соловьев А.В. - ч.2 ст.146; ч.1 ст.273 УК РФ	Уголовное дело ПРЕКРАЩЕНО
Октябрьский районный суд г. Владимира	1-263/2012	06.07.2012	Автономов С.В. - ч.2 ст.146; ч.1 ст.273 УК РФ	Уголовное дело ПРЕКРАЩЕНО
Октябрьский районный суд г. Владимира	1-375/2011	28.10.2011	Кирюхина С.А. - ч.1 ст.273; ч.2 ст.146 УК РФ	Вынесен ПРИГОВОР
Октябрьский районный суд г. Владимира	1-330/2011	14.10.2011	Петров С.В. - ч.2 ст.146; ч.1 ст.273 УК РФ	Уголовное дело ПРЕКРАЩЕНО
Октябрьский районный суд г. Владимира	1-269/2011	01.06.2011	Ковылин Р.И. - ч.1 ст.273; ч.2 ст.146 УК РФ	Уголовное дело ПРЕКРАЩЕНО
Октябрьский районный суд г. Владимира	1-151/2011	12.04.2011	Матвеев В.А. - ч.1 ст.273; ч.2 ст.146 УК РФ	Уголовное дело ПРЕКРАЩЕНО
Октябрьский районный суд г. Владимира	1-57/2011 (1-475/2010;)	26.01.2011	Садовников М.А. - ч.2 ст.146; ч.1 ст.273; ч.1 ст.273 УК РФ	Вынесен ПРИГОВОР
Октябрьский районный суд г. Владимира	1-438/2010	01.12.2010	Некрасов И.В. - ч.1 ст.273; ч.2 ст.146 УК РФ	Уголовное дело ПРЕКРАЩЕНО
Самарская область				
Самарский областной суд	22-190/2017	16.01.17	Востриков Р.Ю. – УК РФ: ст. 138 ч.2; ч.3 ст.272;	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Самарский областной суд			Малинин Д.А. – УК РФ: ст. 33 ч.4 – ст. 138 ч.2; ст. 33 ч.4 – ч.3 ст.272	
Самарский областной суд	22-4362/2016	25.07.2016	Полукаров А.Н. – УК РФ: ч.2 ст.146; ч.2 ст.272; ч.2 ст.273	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Самарский областной суд	22-6029/2014	22.12.2014	Тихонова Н.В. – УК РФ: ч.3 ст.159^6; ч.3 ст.272	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Самарский областной суд	22-4759/2014	20.10.2014	Хоров А.М. – УК РФ: ч.3 ст.159^6; ч.3 ст.272	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Самарский областной суд	22-4263/2014	24.09.2014	Заличев С.А. – УК РФ: ч.1 ст.159^6; ч.2 ст.272	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Самарский областной суд	22-2071/2017	11.04.2017	Куприянов В.С. – УК РФ: ч.2 ст.146; ч.1 ст.273	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Самарский областной суд	22-627/2017	08.02.2017	Елин Е.Н. – УК РФ: п.”в” ч.3 ст.146; ч.2 ст.273	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Самарский областной суд	22-7327/2016	05.12.2016	Григорьев А.Г. – УК РФ: п.”в” ч.3 ст.146; ч.2 ст.273	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Самарский областной суд	22-4524/2016	26.07.2016	Елышев И.О. – УК РФ: п.”в” ч.3 ст.146; ч.2 ст.273	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)

Самарский областной суд	22-6466/2015	09.12.2015	Дундуков Е.Ю. – УК РФ: п.”в” ч.3 ст.146; ч.2 ст.273	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Самарский областной суд	22-1945/2015	22.04.2015	Опарин К.В. – УК РФ: ч.2 ст.146; ч.1 ст.273	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Самарский областной суд	22-1673/2014	21.04.2014	Фролов А.М. – УК РФ: ч.2 ст.146; ч.3 ст.30 – ч.1 ст.273	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Самарский областной суд	22-882/2014	28.02.2014	Костадинов И.Б. – УК РФ: ч.2 ст.146; ч.1 ст.273	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Самарский областной суд	22-648/2013	26.02.2013	Сучков В.К. – УК РФ: п.”в” ч.3 ст.146; ч.1 ст.273	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Автозаводский районный суд г. Тольятти	1-340/2016	13.04.16	Казаков В. В. – ст. 272 ч. 1, ч.2 ст.159^6, ч.1 ст.187УК РФ Васюков А. В. – ч.2 ст.159^6 УК РФ	Вынесен ПРИГОВОР
Промышленный районный суд г. Самары	1-206/2016	04.10.16	Гришин М.И. – ч. 2 ст. 159^6, ч.3 ст. 272 УК РФ	Вынесен ПРИГОВОР
Советский районный суд г. Самары	1-106/2016	17.03.16	Тальянский В.Д. – ч.3 ст.272, ч.3 ст.159^6	Вынесен ПРИГОВОР
Автозаводский районный суд г. Тольятти	1-844/2016	04.08.16	Васенин А.С. – ч.3 ст.272; ч.3 ст.272; ч.3 ст.272; ч.3 ст.272; ч.3 ст.272 УК РФ	Вынесен ПРИГОВОР
Промышленный районный суд г. Самары	1-219/2016	22.04.16	Ковалев С.Н. – ч.3 ст.272; ч.3 ст.272; ч.3 ст.272; ч.3 ст.272; ч.3 ст.272; ч.3 ст.272 УК РФ;	Вынесен ПРИГОВОР
			Нерсисян Г.А. – ч.3 ст.272; ч.3 ст.272; ч.3 ст.272; ч.3 ст.272; ч.3 ст.272; ч.3 ст.272 УК РФ	
Новокуйбышевский городской суд	1-55/2016	25.03.16	Трофимов А.Г. – ч.3 ст.272 УК РФ	Вынесен ПРИГОВОР
Комсомольский районный суд г. Тольятти	1-755/2010	27.10.10	Бражников М.В. – ч.1 ст.272; ч.1 ст.165 УК РФ	Вынесен ПРИГОВОР
Центральный районный суд г. Тольятти	1-573/2013	03.09.13	Абдрашитова И.В. – ч.3 ст.183; ч.3 ст.272; п.«в» ч.3 ст.158 УК РФ	Вынесен ПРИГОВОР
Железнодорожный районный суд г. Самары	1-350/2015	29.12.15	Слизский Д.В. – ч.1 ст.272 УК РФ	Вынесен ПРИГОВОР
Сызранский городской суд	1-387/2016	12.08.16	Вялов О.В. – ч.2 ст. 272; ч.2 ст.273; п.”в” ч.2 ст.158 УК РФ	Вынесен ПРИГОВОР
Сызранский городской суд	1-579/2015	16.11.15	Вялов О.В. – ч.2 ст. 272; п.”в” ч.2 ст.158; ч.2 ст.273 УК РФ	Вынесен ПРИГОВОР
Комсомольский районный суд г. Тольятти	1-227/2012	27.04.12	Панаиотиди А.Н. – ч.2 ст.273; ч.1 ст.272; ч.2 ст. 272; ч.1 ст.273 УК РФ	Вынесен ПРИГОВОР
Свердловская область				
Свердловский областной суд	22-5232/2013	25.04.2013	Семенов А.И. – УК РФ: ч.3 ст.159; ч.4 ст.159; ч.3 ст.30 – ст. 159 ч.2; ч.2 ст.272	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)

Свердловский областной суд	22-8429/2013	18.07.2013	Семенов А.И. – УК РФ: ч.3 ст.30; ст. 159 ч.2; ч.3 ст.159; ч.4 ст.159; ч.2 ст.272	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Свердловский областной суд	22-9067/2015	21.10.2015	Грошко М.В. – УК РФ: ч.3 ст.272	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Свердловский областной суд	22-2331/2017	11.04.2017	Саргсян А.В. – УК РФ: п.”б” ч.3 ст.146; ч.3 ст.272; Тронов С.В. – УК РФ: п.”б” ч.3 ст.146; ч.3 ст.272	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Богдановичский городской суд	1-30/2015	26.08.15	Грошко М.В. – ч.3 ст.272; ст.292 ч.1; ст.292 ч.1; ч.3 ст.272 УК РФ	Вынесен ПРИГОВОР
Верх-исетский районный г. Екатеринбург	1-27/2017 (1-668/2016;)	17.01.17	Аброськин А.М. – ч.3 ст.272 УК РФ	Вынесен ПРИГОВОР
Верх-исетский районный г. Екатеринбург	1-491/2015	02.09.15	Ивасюк В.А. – ч.2 ст.146; ч.1 ст.272; ч.1 ст.272; ч.1 ст.272; ч.1 ст.272; ч.1 ст.273; ч.1 ст.273 УК РФ	Вынесен ПРИГОВОР
Верх-исетский районный г. Екатеринбург	1-540/2016	29.09.16	Кокурин М.А. – ч.1 ст.272; ч.1 ст.272; ч.1 ст.272; ч.1 ст.272; ч.1 ст.272; ч.1 ст.272; ч.1 ст.272; ч.1 ст.272; ч.1 ст.272; ч.2 ст.146 УК РФ	Направлено ПО ПОДСУДНОСТИ (подведомственности)
Кировский районный суд г.Екатеринбург	1-466/2016	28.12.16	Саргсян А.В. – ч.3 ст.272; ч.3 ст.272; ч.3 ст.272; ч.3 ст.272; ч.3 ст.272; ч.3 ст.272; ч.3 ст.272; п.”б” ч.3 ст.146 УК РФ; Тронов С.В. – ч.3 ст.272; ч.3 ст.272; ч.3 ст.272; ч.3 ст.272; ч.3 ст.272; ч.3 ст.272; ч.3 ст.272; п.”б” ч.3 ст.146 УК РФ	Вынесен ПРИГОВОР
Свердловский областной суд	22-2111/2016	15.03.2016	Плотников Ю.В. – УК РФ: п.”в” ч.3 ст.146; ч.1 ст.273	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Свердловский областной суд	22-7203/2015	27.08.2015	Свяжин А.В. – УК РФ: ч.2 ст.146; ч.1 ст.273	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Свердловский областной суд	22-4441/2015	16.06.2015	Марченко Р.В. – УК РФ: п.”в” ч.3 ст.146; ч.1 ст.273	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Свердловский областной суд	22-1718/2015	24.03.2015	Федосов А.С. – УК РФ: ч.2 ст.146; ч.1 ст.273	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Кировградский городской суд	1-105/2016	05.08.16	Томилов Е.В. – ч.2 ст.159^6; ч.2 ст.159^6; ч.2 ст.159^6; ч.2 ст.159^6 УК РФ; Шарапов В.М. – ч.2 ст. 272; ч.2 ст. 272; ч.2 ст. 272; ч.2 ст. 272; ч.2 ст.273; ч.2 ст.273; ч.2 ст.273; ч.1 ст.274; ч.2 ст.159^6; ч.2 ст.159^6; ч.2 ст.159^6; ч.2 ст.159^6; ч.2 ст.273 УК РФ	Вынесен ПРИГОВОР

Магаданская область				
Магаданский городской суд Магаданской области	1-58/2017	18.01.17	Рауцепт О.И. – ч.1 ст.273; п.”в” ч.3 ст.146УК РФ	Вынесен ПРИГОВОР
Магаданский областной суд	22-585/2013	14.08.2013	Оленица С.А. - УК РФ: ч.2 ст.272	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Магаданский областной суд	22-564/2013	07.08.2013	Евсеев А.А. - УК РФ: ч.2 ст.272	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Магаданский областной суд	22-547/2013	31.07.2013	Евсеев А.А. - УК РФ: ч.2 ст.272	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
Магаданский областной суд	22-513/2013	24.07.2013	Евсеев А.А. - УК РФ: п.”а” ч.3 ст.158; ч.2 ст.272	ВЫНЕСЕНО РЕШЕНИЕ (ОПРЕДЕЛЕНИЕ)
г. Москва				
Лефортовский районный суд	1-277/2014	29.09.14	Анисимов А.В. – ч.1 ст.274 УК РФ	ВОЗВРАЩЕНО ПРОКУРОРУ в порядке ст. 237 УПК РФ
Лефортовский районный суд	1-6/2015 (1-401/2014;)	13.01.15	Анисимов А.В. – ч.1 ст.274 УК РФ	Уголовное дело ПРЕКРАЩЕНО
Московский городской суд	10-15427/2014	12.11.14	Анисимов А.В. – ч.1 ст.274 УК РФ	Отменить определение (постановление) полностью, дело вернуть на новое рассмотрение
Бабушкинский районный суд	01-0313/2016	20.09.2016	Чикеев С. Л. (п.”в” ч.3 ст.146; Ч.1 ст.272)	Вынесен ПРИГОВОР
Бабушкинский районный суд	01-0656/2015	13.10.2015	Шестаков Г. П. (ч.1 ст.273; п.”в” ч.3 ст.146; ч.1 ст.272)	Вынесен ПРИГОВОР
Басманный районный суд	01-0036/2017	21.02.2017	Земсков А. А. (ч.2 ст.273; ч.2 ст.146)	Вынесен ПРИГОВОР
Басманный районный суд	01-0465/2016	06.12.2016	Абдалиев А. А. (ч.3 ст.327; Ч.3 ст.327; ч.3 ст.327; ч.2 ст.273; Ч.2 ст.146)	Вынесен ПРИГОВОР
Гагаринский районный суд	01-0160/2017	20.06.2017	Грачунов В. А. (п.”в” ч.3 ст.146; ч.2 ст.273)	Вынесен ПРИГОВОР
Гагаринский районный суд	01-0107/2017	13.04.2017	Адамян Д. Т. (ч.2 ст.273; п.”в” ч.3 ст.146)	Вынесен ПРИГОВОР
Гагаринский районный суд	01-0113/2016	01.04.2016	Лапшин Д. А. (ч.2 ст.273; п.”в” ч.3 ст.146)	Вынесен ПРИГОВОР
Замоскворецкий районный суд г. Москвы	1-2/2016	11.04.2016	Шумарин С. Г. (ч.4 ст.159^6, ч.2 ст.210, ч.3 ст.272), Брагинский И. М. (ч.4 ст.159^6), Федотов Д. Е. (ч.4 ст.159^6, ч.4 ст. 159^6, ч.3 ст.30, ч.2 ст.273, ч.2 ст.210), Пальчевский А. В. (ч.4 ст.159^6, ч.2 ст.210, ч.4 ст.159^6, ч.2 ст.30), Горбунов В. Г. (ч.4 ст.159^6, ч.2 ст.210), Попов В. А. (ч.4 ст.159^6,	Вынесен ПРИГОВОР

			ч.2 ст.210), Кулаков Р. А. (ч.4 ст.159[6], ч.2 ст.210, ч.2 ст.272)	
Измайловский районный суд	01-0605/2016	11.10.2016	Пыхтин В. В. (ч.2 ст.273; ч.2 ст.146)	Вынесен ПРИГОВОР
Измайловский районный суд	01-0267/2016	29.04.2016	Ганеев Р. Р. (ч.2 ст.273; п.”в” ч.3 ст.146)	Вынесен ПРИГОВОР
Измайловский районный суд	01-0215/2016	20.05.2016	Биленко И. А. (п.”в” ч.3 ст.146; Ч.3 ст.273)	Вынесен ПРИГОВОР
Измайловский районный суд	01-0189/2016	01.03.2016	Дубровский И. В. (ч.2 ст.273; п.”в” ч.3 ст.146)	Вынесен ПРИГОВОР
Измайловский районный суд	01-0161/2016	06.05.2016	Зинкин М. Д. (ч.2 ст.273; п.”в” ч.3 ст.146)	Вынесен ПРИГОВОР
Измайловский районный суд	01-0160/2016	12.04.2016	Лукьянец А. О. (п.”в” ч.3 ст.146; ч.2 ст.273)	Вынесен ПРИГОВОР
Измайловский районный суд	01-0158/2016	04.03.2016	Осипов К. Б. (ч.3 ст.273; п.”в” ч.3 ст.146)	Вынесен ПРИГОВОР
Измайловский районный суд	01-0780/2015	21.10.2015	Палякин М. Б. (ч.2 ст.273; п.”в” ч.3 ст.146)	Вынесен ПРИГОВОР
Мещанский районный суд	01-0286/2017	19.05.2017	Филипенко В. И. (ч.2 ст.273)	Вынесен ПРИГОВОР
Люблинский районный суд	01-0335/2017	07.06.2017	Люнгрен И. А. (ч.2 ст.159; Ч.2 ст.272)	Вынесен ПРИГОВОР
Лефортовский районный суд	01-0418/2016	07.12.2016	Саранча Д. А. (ч.1 ст.273; ч.1 ст.273; ч.2 ст.146)	Вынесен ПРИГОВОР
Люблинский районный суд	01-0377/2017	29.06.2017	Харитонов А. А. (ч.2 ст.146; ч.2 ст.273)	Вынесен ПРИГОВОР
Люблинский районный суд	01-0215/2017	16.06.2017	Мастрюков П. А. (ч.2 ст.273; п.”в” ч.3 ст.146)	Вынесен ПРИГОВОР
Люблинский районный суд	01-0170/2017	28.02.2017	Чернышов И. С. (ч.2 ст.273; ч.2 ст.146)	Вынесен ПРИГОВОР
Люблинский районный суд	01-0054/2017	16.01.2017	Коваленко А. Г. (ч.3 ст.273; п.”в” ч.3 ст.146)	Постановление о прекращении производства по делу
Люблинский районный суд	01-0032/2017	21.04.2017	Шаймарданов Т. А. (ч.2 ст.273; ч.2 ст.146)	Вынесен ПРИГОВОР
Люблинский районный суд	01-0031/2017	12.01.2017	Харитонов А. А. (ч.2 ст.273; ч.2 ст.273)	Постановление о возвращении уголовного дела прокурору
Люблинский районный суд	01-0408/2016	02.06.2016	Крысько В. А. (ч.2 ст.273; ч.2 ст.146; п.”в” ч.3 ст.146)	Вынесен ПРИГОВОР
Люблинский районный суд	01-0407/2016	02.06.2016	Давыдов Д. В. (ч.2 ст.273; п.”в” ч.3 ст.146)	Вынесен ПРИГОВОР
Люблинский районный суд	01-0342/2016	02.06.2016	Дергилев И. Ю. (ч.2 ст.146; ч.2 ст.273; п.”в” ч.3 ст.146)	Вынесен ПРИГОВОР
Люблинский районный суд	01-0341/2016	06.05.2016	Воробьев С. (ч.2 ст.146; п.”в” ч.3 ст.146; ч.2 ст.273)	Вынесен ПРИГОВОР
Люблинский районный суд	01-0323/2016	29.04.2016	Панков О. В. (п.”в” ч.3 ст.146; ч.2 ст.146; ч.2 ст.273)	Вынесен ПРИГОВОР
Люблинский районный суд	01-0322/2016	28.04.2016	Озеров Ю. А. (п.”в” ч.3 ст.146; ч.2 ст.273; ч.2 ст.146)	Вынесен ПРИГОВОР
Кузьминский районный суд	01-0605/2017	25.07.2017	Тримаскин К. В. (ч.2 ст.273; п.”в” ч.3 ст.146)	Вынесен ПРИГОВОР

Кузьминский районный суд	01-0526/2017	11.07.2017	Прохорычев Е. А. (п.”в” ч.3 ст.146; ч.2 ст.273)	Вынесен ПРИГОВОР
Кузьминский районный суд	01-0830/2016	27.09.2016	Шапилов В. В. (п.”в” ч.3 ст.146; ч.2 ст.273; ч.2 ст.146)	Вынесен ПРИГОВОР
Кузьминский районный суд	01-0752/2016	02.11.2016	Заболотный А. С. (п.2 ст.273; п.”в” ч.3 ст.146; ч.2 ст.146; ч.2 ст.146; ч. 2 ст. 273 (отм. 07.12.2011))	Вынесен ПРИГОВОР
Кузьминский районный суд	01-0300/2016	14.04.2016	Митин Д. В. (ч.2 ст.273)	Вынесен ПРИГОВОР
Кузьминский районный суд	01-0137/2016	04.03.2016	Мижминскас Е. А. (п.”в” ч.3 ст.146; ч.2 ст.273)	Вынесен ПРИГОВОР
Перовский районный суд	01-0837/2016	07.09.2016	Ерунов З. М. (ч.2 ст.273; п.”в” ч.3 ст.146)	Вынесен ПРИГОВОР
Перовский районный суд	01-0633/2016	01.06.2016	Левашев В. В. (ч.2 ст.273; п.”в” ч.3 ст.146)	Вынесен ПРИГОВОР
Перовский районный суд	01-0488/2016	30.06.2016	Антипов Д. В. (п.”в” ч.3 ст.146; ч.2 ст.273)	Вынесен ПРИГОВОР
Перовский районный суд	01-0299/2016	30.06.2016	Тагиев С. А. О. (ч.3 ст.272; ч.3 ст.272; ч.3 ст.272; ч.3 ст.272; ч.3 ст.272; ч.3 ст.272), Асроров Б. З. (ч.3 ст.272; ч.3 ст.272; ч.3 ст.272; ч.3 ст.272; ч.3 ст.272; ч.3 ст.272)	Вынесен ПРИГОВОР

Приложение 3

Таблица анализа использования понятий «информация», «сообщения», «сведения», «данные» в Уголовном кодексе Российской Федерации

Информация	Сообщение	Сведения	Данные		Наименование статьи
Общая часть					
1					Статья 33. Виды соучастников преступления
		1			Статья 63^1. Назначение наказания в случае нарушения досудебного соглашения о сотрудничестве
1					Статья 76^1. Освобождение от уголовной ответственности по делам о преступлениях в сфере экономической деятельности
Особенная часть				Раздел	Особенная часть
		1		Преступления против личности	Статья 128^1. Клевета
		1			Статья 137. Нарушение неприкосновенности частной жизни
	1				Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений

1					Статья 138[1]. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации
1					Статья 140. Отказ в предоставлении гражданину информации
		1			Статья 142[1]. Фальсификация итогов голосования
1					Статья 144. Воспрепятствование законной профессиональной деятельности журналистов
		1			Статья 147. Нарушение изобретательских и патентных прав
		1		Преступления в сфере экономики	Статья 159[1]. Мошенничество в сфере кредитования
		1			Статья 159[2]. Мошенничество при получении выплат
1					Статья 159[6]. Мошенничество в сфере компьютерной информации
		1			Статья 163. Вымогательство
		1			Статья 170. Регистрация незаконных сделок с недвижимым имуществом
		1	1		Статья 170[1]. Фальсификация единого государственного реестра юридических лиц, реестра владельцев ценных бумаг или системы депозитарного учета
		1			Статья 170[2]. Внесение заведомо ложных сведений в межевой план, технический план, акт обследования, проект межевания земельного участка или земельных участков либо карту-план территории
		1			Статья 172[1]. Фальсификация финансовых документов учета и отчетности финансовой организации
		1	1		Статья 173[1]. Незаконное образование (создание, реорганизация) юридического лица
		1	1		Статья 173[2]. Незаконное использование документов для образования (создания, реорганизации) юридического лица
		1			Статья 176. Незаконное получение кредита
		1			Статья 179. Принуждение к совершению сделки или к отказу от ее совершения
		1			Статья 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну
1					Статья 185. Злоупотребления при эмиссии ценных бумаг
1					Статья 185[1]. Злостное уклонение от раскрытия или предоставления информации, определенной законодательством Российской Федерации о ценных бумагах
		1			Статья 185[2]. Нарушение порядка учета прав на ценные бумаги
		1			Статья 185[3]. Манипулирование рынком
	1	1			Статья 185[5]. Фальсификация решения общего собрания акционеров (участников) хозяйственного общества или решения совета директоров (наблюдательного совета) хозяйственного общества

1					Статья 185[6]. Неправомерное использование инсайдерской информации
1					Статья 187. Неправомерный оборот средств платежей
1					Статья 189. Незаконные экспорт из Российской Федерации или передача сырья, материалов, оборудования, технологий, научно-технической информации, незаконное выполнение работ (оказание услуг), которые могут быть использованы при создании оружия массового поражения, вооружения и военной техники
1					Статья 193. Уклонение от исполнения обязанностей по репатриации денежных средств в иностранной валюте или валюте Российской Федерации
		1			Статья 193[1]. Совершение валютных операций по переводу денежных средств в иностранной валюте или валюте Российской Федерации на счета нерезидентов с использованием подложных документов
		1			Статья 195. Неправомерные действия при банкротстве
		1			Статья 198. Уклонение от уплаты налогов и (или) сборов с физического лица
		1			Статья 199. Уклонение от уплаты налогов и (или) сборов с организации
1				Преступления против общественной безопасности и общественного порядка	Статья 205[1]. Содействие террористической деятельности
		1			Статья 215[4]. Незаконное проникновение на охраняемый объект
1					Статья 237. Сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей
1	1	1	1		Статья 272. Неправомерный доступ к компьютерной информации
1					Статья 273. Создание, использование и распространение вредоносных компьютерных программ
1					Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей
1					Статья 274[1]. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации
		1		Преступления против государственной власти	Статья 275. Государственная измена
		1			Статья 276. Шпионаж
		1			Статья 283. Разглашение государственной тайны
		1			Статья 283[1]. Незаконное получение сведений, составляющих государственную тайну
		1			Статья 284. Утрата документов, содержащих государственную тайну
		1			Статья 285[3]. Внесение в единые государственные реестры заведомо недостоверных сведений
1					Статья 287. Отказ в предоставлении информации Федеральному Собранию Российской Федерации или Счетной палате Российской Федерации
		1			Статья 292. Служебный подлог
		1			Статья 292[1]. Незаконная выдача паспорта гражданина Российской Федерации, а равно внесение заведомо ложных

					сведений в документы, повлекшее незаконное приобретение гражданства Российской Федерации
			1		Статья 310. Разглашение данных предварительного расследования
		1			Статья 311. Разглашение сведений о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса
		1			Статья 320. Разглашение сведений о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа
		1		Преступления против мира и безопасности человечества	Статья 354[1]. Реабилитация нацизма
19	3	37	5		

Примечание: проставленный в строке символ «1» свидетельствует о наличии термина, указанного в одном из столбцов первой строки таблиц, в исследуемой статье УК РФ.

Приложение 4

Таблица анализа использования понятий «средства массовой информации» и «информационно-телекоммуникационные сети» в УК РФ

Средства массовой информации	**Информационно-телекоммуникационные сети**	**Раздел УК РФ**	**Наименование статьи УК РФ**
1		Преступления против личности	*Статья 137. Нарушение неприкосновенности частной жизни*
1	1		Статья 110[1]. Склонение к совершению самоубийства или содействие совершению самоубийства.
1	1		Статья 110[2]. Организация деятельности, направленной на побуждение к совершению самоубийства.
1	1	Преступления против общественной безопасности	Статья 228.1. Незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих

		и общественного порядка	наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества
1	1		Статья 242. Незаконные изготовление и оборот порнографических материалов или предметов
	1		Статья 242.1. Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних
	1		Статья 242.2. Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов
1	1	Преступления против государственной власти	Статья 280. Публичные призывы к осуществлению экстремистской деятельности
1	1		Статья 280.1. Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации
1	1		Статья 282. Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства
1		Преступления против мира и безопасности человечества	Статья 354. Публичные призывы к развязыванию агрессивной войны
1			*Статья 354.1. Реабилитация нацизма*
Итого: 10	Итого: 9		

Примечание: проставленный в строке символ «1» свидетельствует о наличии термина, указанного в первой строке столбца приведенной таблицы, в исследуемой статье УК РФ.

Приложение 5

Данные о судимости лиц женского пола за преступления в сфере компьютерной информации

Год	Кол-во осужденных лиц женского пола
2013 г.	15
2014 г.	9
2015 г.	9
2016 г.	10

Приложение 6

Данные о наличии образования у лиц, осужденных за преступления в сфере компьютерной информации

Год	Высшее профессиональное – доля среди общего числа осужденных, в %	Среднее профессиональное – доля среди общего числа осужденных, в %	Среднее общее – доля среди общего числа осужденных, в %	Основное общее, начальное или нет образования – доля среди общего числа осужденных, в %
2013	92 – 34%	85 – 32%	76 – 28%	15 – 6%
2014	73 – 34%	76 – 35%	57 – 26%	12 – 5%
2015	70 – 30%	88 – 38%	62 – 26%	15 – 6%
2016	72 – 39%	54 – 25%	49 – 26%	10 – 5%

Приложение 7

Данные о возрасте лиц, осужденных за преступления в сфере компьютерной информации

Год	Всего осуждено лиц (по основной статье)	14-17 лет	18-24 лет	25-29 лет	30-49 лет	50 лет и старше
2013	268	5	111	70	78	4
2014	218	1	79	56	77	5
2015	235	0	93	72	63	7
2016	185	3	65	45	66	6

Приложение 8

Данные о лицах, совершивших преступления в сфере компьютерной информации группой лиц и организованной группой лиц

Год	Осуждено лиц, совершивших преступления группой лиц.	В том числе организованной группой	Всего осуждено лиц по гл. 28 УК РФ (по основной статье)	Доля лиц, совершивших преступления группой лиц, среди лиц, осужденных по гл. 28 УК РФ (по осн. ст.)
2013	14	2	268	5%
2014	12	1	218	6%
2015	14	2	235	6%
2016	12	2	185	6%

Приложение 9

Данные о лицах, осужденных за неоконченные преступления в сфере компьютерной информации

Год	272 УК	273 УК	274 УК	Всего неоконченных преступлений	Всего совершено преступлений по гл. 28 УК РФ
2013	-	1 – по ч. 1 ст. 273	14 – по ч. 2 ст. 273	22	268
2014	4 – по ч. 3 ст. 272	4 – по ч. 1 ст. 273	4 – по ч. 2 ст. 273	12	218
2015	1 – по ч. 2 ст. 272	1 – по ч. 1 ст. 273	9 – по ч. 2 ст. 273	11	235
2016	-	-	3 – по ч. 3 ст. 273	3	185