На правах рукописи

Челноков Владислав Валерьевич

КОМПЬЮТЕРНАЯ ИНФОРМАЦИЯ КАК ПРЕДМЕТ ПРЕСТУПЛЕНИЯ В ОТЕЧЕСТВЕННОМ УГОЛОВНОМ ПРАВЕ

Специальность 12.00.08 - Уголовное право и криминология,
уголовно-исполнительное право

Автореферат
диссертации на соискание учёной степени
кандидата юридических наук

Екатеринбург – 2013

Диссертация выполнена на кафедре уголовного права Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Уральская государственная юридическая академия»

Научный руководитель: доктор юридических наук, профессор,
Незнамова Зинаида Александровна

Официальные оппоненты: доктор юридических наук, профессор,
заведующий кафедрой уголовного права и криминологии юридического факультета ФГБОУ ВПО «Самарский государственный университет»
Клёнова Татьяна Владимировна

кандидат юридических наук,
заведующий кафедрой уголовного права Екатеринбургского филиала ФГБОУ ДПО «Институт повышения квалификации Следственного комитета Российской Федерации»
Яшков Сергей Александрович

Ведущая организация: ФГКОУ ВПО «Институт ФСБ России (г. Нижний Новгород)»

Защита состоится 10 октября 2013 года в 13 часов 00 минут на заседании диссертационного совета Д 212.282.03 при ФГБОУ ВПО «Уральская государственная юридическая академия» по адресу: 620137, г. Екатеринбург, ул. Комсомольская, д. 21, зал ученого совета.

С диссертацией можно ознакомиться в библиотеке Уральской государственной юридической академии.

Автореферат разослан « » _____ 2013 года

Учёный секретарь
диссертационного совета
доктор юридических наук,
профессор З.А. Незнамова

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертационного исследования. Современное состояние общества характеризуется высокими темпами научно-технического прогресса. К его проявлениям можно отнести непрерывно растущий уровень автоматизации практически всех сфер человеческой деятельности. Основу такой автоматизации составляют электронные вычислительные машины (ЭВМ) или, как их сейчас называют, компьютеры. Поскольку функционирование ЭВМ обусловлено процессами обработки информации (вычислений), то процессы автоматизации коснулись, прежде всего, информационной сферы общества.

Новый импульс развитию информационной сферы в конце XX века дало появление компьютерных сетей, особенно открытой глобальной компьютерной сети Интернет. Благодаря компьютерным сетям финансовая и торговая сферы деятельности вышли на качественно новый уровень. Сеть Интернет не только предоставила людям возможности свободной связи по всему миру, но и стала всеобъемлющим информационным ресурсом, не имеющим аналогов. Она постоянно развивается, обеспечивая своих пользователей новыми технологиями доступа и обмена информацией. В этих условиях сформировался новый безбумажный оборот информации, носителями которой стали ЭВМ, её средства (машинные носители информации) и компьютерные сети. А сама информация, обрабатываемая ЭВМ, передаваемая по компьютерным сетям и хранимая на машинных носителях, получила название компьютерной информации.

Вместе с тем развитие информационных технологий открыло и новые возможности для совершения преступлений с помощью ЭВМ — компьютерных преступлений. При этом использование ЭВМ возможно как при совершении «традиционных» преступлений, например, мошенничества, распространения порнографии, подделки документов или денежных знаков, так и при совершении принципиально новых общественно опасных деяний с компьютерной информацией, до этого не известных уголовному праву.

Именно для устранения этого законодательного пробела в 1996 году в УК РФ была введена глава 28 «Преступления в сфере компьютерной информации», содержащая ст. 272 – 274.

С момента принятия УК РФ прошло уже 16 лет, и можно подвести некоторые итоги. Согласно статистическим данным МВД России количество зарегистрированных преступлений в сфере компьютерной информации неуклонно росло до 2004 г — 13 723, затем снизилось в 2007 г. до 7236, в 2009 г. достигло 11 636, в 2010 г. — 7398, а в 2011 г. резко снизилось до 2698, то есть практически до уровня 2001 г. — 2133, и в 2012 г. осталось примерно на том же уровне — 2820[1].

Некоторые авторы причину такого резкого сокращения зарегистрированных преступлений объясняют их высокой латентностью[2]. Действительно, сотрудники зарубежных и отечественных правоохранительных органов, занимающиеся расследованием подобных преступлений, отмечают, что от 85 до 97 % компьютерных атак[3] остаются незамеченными[4]. Вместе с тем дальнейшее развитие компьютерных технологий, в том числе, на мобильных телефонных аппаратах, а также статистика антивирусных компаний, отмечающих устойчивый ежегодный рост компьютерных атак, позволяют усомниться в значительном уменьшении преступлений в сфере компьютерной информации. Так, по данным Лаборатории Касперского для проведения 1 595 587 670 атак через сеть Интернет злоумышленники воспользовались 6 537 320 уникальными ЭВМ, что на два с половиной миллиона больше, чем в 2011 году. ЭВМ (серверы), на которых был размещен вредоносный код, были обнаружены практически во всех странах мира. 96,1% всех зафиксированных в сети Интернет атак были произведены с ЭВМ расположенных в интернет-пространстве двадцати стран. Количество атак с интернет-ресурсов РФ достигло

[1] Статистика преступлений // Министерство внутренних дел Российской Федерации. Официальный сайт URL: http://www.mvd.ru/presscenter/statistics/reports (дата обращения: 17.02.2013).

[2] Косынкин А.А. Преодоление противодействия расследованию преступлений в сфере компьютерной информации. Автореф. дисс. канд. юрид. наук. — Саратов ФГБОУ ВПО «Саратовская государственная юридическая академия», 2012. С. 3.

[3] Компьютерная атака — целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 374-ст) // Официальное издание Федерального агентства по техническому регулированию и метрологии. — М.: Стандартинформ, 2007.

[4] Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями: Пер. с англ. — М.: Мир, 1999. С. 18; Фио-Фио-Сам. Полицейское управление «К» предложило запретить анонимные выступления в Интернете // Российская газета. URL: http://www.rg.ru/2011/12/08/ moshkov.html (дата обращения: 12.12.2012).

317 697 806, это 2-е место после США и составляет 19,6 % (+5 % по сравнению с прошлым годом) от всех зафиксированных атак в мире[5].

Статистика МВД России указывает на достаточно высокий уровень раскрываемости таких преступлений: в 2009 г. из 11 636 преступлений раскрыто 11 296 (97%), в 2010 г. из 7 398 раскрыто 6 804 (92%), в 2011 г. из 2 698 раскрыто 2 687 (99%), в 2012 г. из 2 820 раскрыто 2 425 (86%)[6]. Между тем раскрываемость более «явных» (нелатентных) преступлений, по которым обязательно предварительное следствие, таких как кража и хулиганство с квалифицирующими признаками, существенно ниже. Так, в 2012 г. из 678 зарегистрированных случаев хулиганства (ч. 2 ст. 213 УК РФ) раскрыто только 283 (42%), из 669 562 зарегистрированных краж (ч. 2–4 ст. 158 УК РФ) раскрыто 239 474 (36%)[7]. Очевидно, что раскрываемость преступлений в сфере компьютерной информации не может быть в 2–3 раза выше раскрываемости краж и хулиганства и достигать 99%.

Вероятно, органы МВД России имели возможность регистрировать только те преступления в сфере компьютерной информации, по которым уже имелись необходимые для их раскрытия сведения. Кроме того, резкое уменьшение количества зарегистрированных в 2011 г. преступлений в сфере компьютерной информации приходится на период реформирования органов МВД России и переаттестации их сотрудников. Таким образом, оценивать уровень преступности в сфере компьютерной информации по официальной статистике МВД России, по меньшей мере, некорректно.

Высокотехнологичный характер совершения преступлений в сфере компьютерной информации значительно осложняет не только их расследование, но и квалификацию по ст. 272–274 УК РФ. Как в теории, так и в практике применения ст. 272–274 УК РФ выявились существенные противоречия. Среди основных их причин можно выделить следующие: не совсем удачные конструкции норм о преступлениях в сфере компьютерной информации, неверное их толкование, не соответствующее действительности представление о значении указанных норм в охране благ и интересов. Особую актуальность тема приобретает в условиях вступления в силу в декабре 2011 г. новых редакций ст. 272–274 УК РФ, в которых не до конца устранены недостатки старых редакций.

---

[5] Костин Раю, Дэвид Эмм. Развитие угроз в 2012 году. Kaspersky Security Bulletin 2012 // Securelist. URL: http://www.securelist.com/ru/analysis/208050777/Kaspesky_Security_Bulletin_2012_Razvitie_ugroz_v_2012_godu (дата обращения: 15.01.2013).

[6] Статистика преступлений // Министерство внутренних дел Российской Федерации. Там же.

[7] Там же.

С учётом всех этих обстоятельств необходимо исследовать действующее уголовное законодательство о преступлениях в сфере компьютерной информации и проанализировать практику его применения. Указанными причинами и обусловлен выбор темы настоящего диссертационного исследования.

Степень научной разработанности проблемы. Уголовно-правовые аспекты преступлений в сфере компьютерной информации являлись предметом диссертационных исследований С.Д. Бражника, У.В. Зининой, Д. А. Зубовой, В.С. Карпова, А.А. Косынкина, Т.М. Лопатиной, В.Ю. Максимова, В.В. Малыковцева, Е.А. Маслаковой, И.А. Сало, М.В. Старичкова, В.Г. Степанова-Егаянца, В.В. Суслопарова, Т.Л. Тропиной, С.С. Шахрая и др.

Между тем ряд вопросов, связанных с компьютерной информацией как с предметом преступления, до сих пор не получил должного рассмотрения в научных трудах. Кроме того, научные выводы указанных авторов были сделаны до вступления в силу в декабре 2011 г. новых редакций статей гл. 28 УК РФ, в которых были изменены понятия предметов преступлений в сфере компьютерной информации.

Объектом исследования являются общественные отношения в сфере обращения компьютерной информации, блага и интересы, которым может быть причинён ущерб преступными посягательствами, предметом которых является компьютерная информация, а также права отдельных лиц, общества и государства, связанные с безопасностью обработки компьютерной информации и нормальным функционированием ЭВМ, информационных систем и информационно-телекоммуникационных сетей.

Предметом исследования выступают:

- уголовно-правовые нормы о преступлениях в сфере компьютерной информации, содержащиеся в отечественном и зарубежном законодательстве;
- нормы других отраслей права, регулирующие информационные отношения;
- нормы международного права, связанные с компьютерными преступлениями;
- научные публикации, диссертационные исследования по уголовно-правовой, криминалистической и компьютерно-технической тематике;
- материалы следственной и судебной практики по делам о преступлениях, ответственность за которые предусмотрена ст. 272 и 273 УК РФ;
- результаты социологических исследований сотрудников правоохранительных органов;

- статистические данные о преступлениях в сфере компьютерной информации.

Цели и задачи диссертационного исследования. Целью данного исследования является определение научного понятия и признаков компьютерной информации как предмета преступления на основе изучения компьютерно-технической, криминалистической и уголовно-правовой литературы, законодательства РФ и иностранных государств, анализа практики применения отечественных составов преступления, предметом которых является компьютерная информация.

Достижение этой цели обеспечивается решением следующих **задач**:

- проанализировать современные знания и нормативные понятия для выявления существенных признаков компьютерной информации и компьютерных программ (программ для ЭВМ);
- исследовать компьютерную информацию как предмет преступления, раскрыть её особенности;
- изучить практику применения составов преступлений, в которых компьютерная информация является предметом преступления;
- провести оценку общественной опасности криминализированных деяний с компьютерной информацией;
- разработать конкретные рекомендации по совершенствованию составов преступлений, предметом которых является компьютерная информация.

Методологическая основа исследования. Методологическую основу исследования составляет совокупность общенаучных и частно-научных методов. В числе общенаучных методов были использованы: диалектический метод, метод анализа и синтеза составных частей, логический метод. Применялись также и специальные методы (сравнительного правоведения, исторический, социологический).

Теоретической основой диссертационного исследования стали труды учёных в области уголовного и информационного права, компьютерной криминалистики и информационных технологий. Учение о предмете преступления рассматривается в научных трудах М.П. Бикмурзина, С.Ф. Кравцова, А.Н. Круглевского, В.Н. Кудрявцева, И.В. Кузнецова, А.В. Наумова, Г.П. Новосёлова, А.А. Пионтковского, Н.Д. Сергиевского, Н.С. Таганцева, В.Я. Тация, А.Н. Трайнина, А.В. Шульги и др. Правовым проблемам информатизации российского общества и защиты информации посвящены работы

В.В. Бакланова, В.Б. Вехова, А.Г. Волеводза, В.А. Копылова, В.В. Крылова, В.Д. Курушина, В.А. Мазурова, М.Э. Пономарёва, С.А. Яшкова и др.

Нормативную основу диссертационного исследования составили Конституция РФ, Уголовный кодекс РФ, Гражданский кодекс РФ, Налоговый кодекс РФ, Семейный кодекс РФ, Кодекс РФ об административных правонарушениях, ФЗ «Об информации, информационных технологиях и о защите информации», Закон РФ «О государственной тайне», ФЗ «О коммерческой тайне» и др. нормативные акты.

Изучены связанные с компьютерной информацией уголовные нормы США, Германии, Великобритании, Испании, Финляндии, Франции, Эстонии, государств СНГ, а также Конвенция о киберпреступности и Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации.

Эмпирическую базу диссертации составляет следственная и судебная практика по уголовным делам с квалификацией по ст. 272 и 273 УК РФ за период с 1999 г. по 2012 г. В работе использованы материалы 120 находящихся в производстве и завершённых уголовных дел, в том числе из архивов Октябрьского и Чкаловского районных судов г. Екатеринбурга, Тагилстроевского районного суда г. Нижнего Тагила и с Интернет-портала государственной автоматизированной системы «Правосудие». В процессе исследования по тематике преступлений в сфере компьютерной информации проведены опросы 85 следователей и оперативных работников органов безопасности. Также при подготовке диссертации использовались материалы практического опыта автора, приобретённого в ходе многолетней профессиональной деятельности, связанной с проведением компьютерных криминалистических экспертиз и исследований компьютерной техники, в том числе по уголовным делам в сфере компьютерной информации.

Научная новизна диссертации состоит в том, что работа представляет собой одно из специальных монографических исследований института уголовной ответственности за преступления в сфере компьютерной информации по российскому уголовному законодательству в условиях их недавнего изменения. Выработаны предложения по изменению и дополнению диспозиций уголовных норм гл. 28 УК РФ.

Научная новизна также определяется **основными положениями, выносимыми на защиту**:

1. Критикуется определение компьютерной информации, приведённое в приложении 1 новой редакции ст. 272 УК РФ. Указывается на то, что оно корректно только для состава данной статьи. Однако применительно к ст. 273 УК РФ данное определение неоправданно «сужает» понятие компьютерной информации, тем самым декриминализируя распространение вредоносной компьютерной информации на машинных носителях информации. Предлагается авторское понятие компьютерной информации для целей ст. ст. 272 и 273 УК РФ.

2. Выделяются обязательные и факультативные признаки охраняемой законом компьютерной информации как предмета преступления, предусмотренного ст. 272 УК РФ.

3. Отстаивается тезис о том, что для охраны компьютерной информации от неправомерного доступа большее значение имеют меры по её защите, чем формальная охрана законом. В уголовно-правовой защите в первую очередь нуждаются такие обладатели компьютерной информации, которые предприняли реальные меры по обеспечению её безопасности. Вносится предложение о криминализации неправомерного доступа не «к охраняемой законом компьютерной информации», а «сопряжённого с нейтрализацией средств её защиты».

4. Даётся понятие нейтрализации средств защиты компьютерной информации.

5. Доказывается необоснованность исключения из ст. 272 и 273 УК РФ такого последствия неправомерного доступа к компьютерной информации и соответственно выполнения вредоносной программы, как нарушение работы ЭВМ, систем ЭВМ или их сетей. Такие общественно опасные нарушения могут иметь место без явных признаков уничтожения, блокирования, модификации или копирования компьютерной информации, предусмотренных в указанных в статьях. В этой связи вносится предложение о криминализации компьютерного саботажа — умышленного уничтожения или повреждения компьютерной информации либо нарушения работы или выведения из строя ЭВМ, информационных систем или информационно-телекоммуникационных сетей.

6. Утверждается, что общественную опасность в виде угрозы нарушения конфиденциальности информации представляет неправомерное копирование компьютерной информации (без признаков неправомерного доступа к ней), не предусмотренное УК РФ.

7. Обосновывается необходимость криминализации неправомерной модификации компьютерной информации, причинившей значительный ущерб и (или) существенный

вред правам и законным интересам граждан или организаций либо охраняемым законом интересам общества или государства.

8. Критикуется определение программы для ЭВМ, представленное в ст. 1261 ГК РФ. Обосновывается неприемлемость использования данного определения при квалификации деяний по ст. 273 УК РФ. При этом предлагается руководствоваться определением программы для ЭВМ, приведённым в ГОСТ 15781-90 «Обеспечение систем обработки информации программное»[8].

9. Доказывается, что несанкционированное уничтожение, блокирование, модификация или копирование компьютерной информации далеко не всегда можно признать в качестве общественно опасных последствий или назначения вредоносной компьютерной информации. Таковыми следует считать значительный ущерб и (или) существенный вред правам и законным интересам граждан или организаций либо охраняемым законом интересам общества или государства. Предлагаются соответствующие изменения в ст. 272 и 273 УК РФ.

10. Обосновывается необходимость указания в ст. 273 УК РФ на исключение из числа вредоносных компьютерных программ или иной компьютерной информации, предназначенных для использования или используемых в оперативно-розыскной, разведывательной или контрразведывательной деятельности, либо для осуществления производства по делу об административном правонарушении, производства дознания, предварительного следствия или осуществления правосудия, если они создаются, распространяются и используются лицами, наделёнными соответствующими законными полномочиями.

Теоретическая значимость исследования. Содержащиеся в диссертационной работе теоретические положения и выводы, направленные на развитие и совершенствование общей теории правового регулирования отношений в сфере компьютерной информации, могут использоваться для дальнейших исследований, связанных с проблемой уголовной ответственности за преступления, совершённых с использованием компьютерных технологий.

[8] ГОСТ 15781-90 «Обеспечение систем обработки информации программное» (утв. и введен в действие постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 27 авг. 1990 г. № 2767) // Официальное издание, Единая система программной документации: Сб. ГОСТов. — М.: Стандартинформ, 2005. П. 1 табл. 1.

Практическая значимость выводов и предложений диссертационного исследования. Полученные результаты могут быть использованы в правотворческой деятельности по совершенствованию уголовно-правовых норм об ответственности за преступления в сфере компьютерной информации и связанные с ними правонарушения; при квалификации преступных деяний; при разработке методик выявления и пресечения рассматриваемых преступлений; в учебном процессе.

Апробация результатов исследования. Диссертация выполнена на кафедре уголовного права Уральской государственной юридической академии, где проводилось её рецензирование и обсуждение. Основные положения и выводы диссертационного исследования изложены в научных статьях и других публикациях, докладывались на заседании кафедры уголовного права, на Всероссийской научно-практической конференции «Проблемы правового и организационно-технического обеспечения информационной безопасности России» в Екатеринбурге в 2001 г., на Всероссийской научно-практической конференции «Информационная безопасность региона» в Челябинске в 2004 г., на Международной научно-практической конференции «Уголовная политика в сфере информационной безопасности Российской Федерации» в г. Екатеринбурге в 2007 г. Результаты исследования используются в учебном процессе в Уральском федеральном университете имени первого Президента России Б.Н. Ельцина и в Институте ФСБ России (г. Екатеринбург).

Структура диссертации отвечает основной цели и предмету исследования. Работа состоит из введения, трёх глав, содержащих девять параграфов, заключения, приложений, библиографического списка, включающего 217 наименований.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы диссертации, определяются объект, предмет, цели и задачи исследования, его методологическая основа, отражается научная новизна работы с указанием положений, выносимых на защиту, отмечается теоретическая и практическая значимость диссертации, приводятся сведения об апробации результатов исследования, его структуре.

Первая глава «Уголовно-правовая природа компьютерной информации» состоит из трёх параграфов.

Первый параграф «Развитие взглядов на предмет преступления в отечественной науке уголовного права» посвящён рассмотрению эволюции понятия предмета преступления; даётся обзор точек зрения российских правоведов по указанной проблеме.

До начала XX века объект и предмет преступления трактовались как синонимичные понятия. Одним из первых о необходимости выделения предмета воздействия преступника заявил Н.С. Таганцев[9]. В советское время дальнейшее развитие учения о предмете преступления можно условно разделить на два основных направления – в зависимости от места предмета преступления в составе преступления: 1) предмет преступления — признак состава, характеризующий объективную сторону преступления; 2) предмет преступления — признак состава, характеризующий объект преступления.

К последователем первого направления диссертант относит А.Н. Трайнина, Б.А. Куринова, А.А. Пионтковского, А.Н. Васильева, М.П. Михайлова и М.П. Бикмурзина.

Второе направление, в котором предмет преступления рассматривался как признак объекта преступления, поддерживалось подавляющим большинством юристов. Соискатель отмечает, что в его рамках взгляды на предмет преступления менялись от представления как вещи материального мира до включения в его состав также нематериальных благ как предметов нарушаемых общественных отношений; людей — субъектов общественных отношений; поведения людей как содержания общественных отношений.

[9] Таганцев Н.С. Русское уголовное право. Лекции. Часть Общая. Т.1. – СПб., 1902 // М. : «Наука», 1994. — С. 32.

Автор указывает, что сегодня некоторые правоведы предлагают расширить объём понятия предмета преступления путём включения в него также интеллектуальных ценностей и информации. Рассматривая последнюю как предмет преступления, автор наряду с другими отмечает, что информация может представлять как ценность, так и общественную опасность.

Предметом, представляющим ценность, она является в тех составах преступлений, которые обеспечивают её уголовно-правовую охрану: это сведения, составляющие государственную тайну (ст. 275, 276, 283, 283.1 УК РФ), сведения, составляющие коммерческую тайну (ст. 183 УК РФ), сведения, составляющие тайну переписки, телефонных переговоров и иных сообщений (ст. 138 УК РФ). Такие сведения, безусловно, можно признать интересами или благами, охраняемыми уголовным законом, что не противоречит традиционной точке зрения о предмете преступления как признаке объекта преступления.

Вместе с тем соискатель отмечает, что информация как предмет, представляющий общественную опасность, нашла своё отражение в УК РФ в качестве публичных призывов к осуществлению экстремисткой деятельности (ст. 280 УК РФ), публичных призывов к осуществлению террористической деятельности (ст. 205.1 УК РФ), клеветы (ст. 128.1 УК РФ), где она уже не относится к охраняемым уголовным законом отношениям, интересам или благам, что, в свою очередь, не позволяет признать её признаком объекта преступления.

Автор поддерживает точку зрения о том, что предмет преступления должен признаваться признаком объективной стороны преступления, и которую на его взгляд удачно выразил М.П. Бикмурзин: «Предмет преступления является признаком, характеризующим объективную сторону состава преступления, но не его объект. При ином решении вопроса о расположении предмета преступления в системе признаков состава преступления, без определённой роли в составе остаются предметы, чуждые объекту преступного посягательства, — опасные вещи, недостоверная информация, предметы подкупа. В современном уголовном законодательстве эти предметы без какого-либо обоснования включаются в объём понятия предмета преступления, что входит в явное противоречие с положением о месте предмета преступления в объекте преступления.

Предлагаемое перемещение предмета преступления в объективную сторону преступления позволяет разрешить это противоречие»[10].

Подтверждением этой позиции может служить существование компьютерной информации как опасного предмета преступления, который не относится к объекту уголовно-правовой охраны. Таким предметом преступления, например, являются вредоносная компьютерная программа или иная вредоносная компьютерная информация, чуждые информационной безопасности.

В дальнейшем предлагается рассматривать компьютерную информацию как предмет преступления именно во взаимосвязи с такими элементами объективной стороны преступления, как орудия и средства совершения преступления, в качестве которых выступают ЭВМ и их носители информации.

Во втором параграфе «Понятие компьютерной информации» автор критикует данное законодателем в примечании 1 новой (с декабря 2011 г.) редакции ст. 272 УК РФ, определение компьютерной информации, под которой следует понимать «сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи».

В ЭВМ информация посредством электрических сигналов передаётся между устройствами её хранения (памятью) и арифметико-логическим устройствами (процессорами). Электрические сигналы могут обрабатываться и передаваться в функционирующей (работающей) ЭВМ и в проводных электрических линиях связи компьютерной сети. То есть законодатель фактически признаёт, что компьютерная информация имеет место только в работающих ЭВМ и проводном канале связи. Однако упоминание в примечании 1 к ст. 272 УК РФ о хранении электрических сигналов, на взгляд автора, некорректно, поскольку процесс хранения не свойственен сигналу.

Хранение информации в ЭВМ, особенно долговременное энергонезависимое (без электрического тока), основано в настоящее время на следующих физических принципах: полупроводниковых, магнитных, электромагнитных, оптических. Электрические сигналы отсутствуют на оптических дисках, в обесточенных накопителях на жёстких магнитных

[10] Бикмурзин М.П. Предмет преступления: теоретико-правовой анализ. — М.: Издательство «Юрлитинформ», 2006. С. 167.

дисках (НЖМД)[11], флэш-носителях (накопителях)[12], в радиоволнах и оптоволоконных линиях связи.

Таким образом, в соответствии с новым легальным определением компьютерной информации к предметам преступлений, предусмотренных ст. 272 и 273 УК РФ, относятся данные, обрабатываемые на работающей ЭВМ или передаваемые по проводным электрическим линиям связи. При этом те же данные, хранящиеся в выключенной ЭВМ, на оптическом диске или на обесточенных НЖМД или флэш-носителе, а равно передаваемые по радиоканалу или по оптоволоконным линиям связи, в соответствии с примечанием 1 к ст. 272 УК РФ уже нельзя признать компьютерной информацией. Вместе с тем согласно указанному определению можно признать компьютерной информацию, передаваемую по телефонным проводным линиям связи, которая может не иметь никакого отношения к ЭВМ.

Также отмечается, что трактовка компьютерной информации в соответствии с примечанием 1 к ст. 272 УК РФ требует от правоприменителей при квалификации деяний в сфере компьютерной информации разрешения вопроса о наличии на носителях информации ЭВМ сведений (сообщений, данных), представленных в виде электрических сигналов.

Определение компьютерной информации в предыдущей редакции ст. 272 УК РФ (до декабря 2011 г.) было лишено указанных недостатков. В нём к компьютерной была отнесена информация на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети.

Предлагается в примечании 1 к ст. 272 УК РФ использовать следующее определение компьютерной информации: «Компьютерная информация — это информация, находящаяся в памяти ЭВМ (информационной системы), на носителе информации в форме, доступной для обработки на ЭВМ (информационной системе), или передающаяся по информационно-телекоммуникационной сети».

В заключение второго параграфа автор приходит к выводу, что невозможность действий с компьютерной информацией без ЭВМ и передачи и хранения её без машинных

[11] Во включенном состоянии НЖМД электрические сигналы проходят через его контроллер управления, представляющий собой специализированную ЭВМ, предназначенную исключительно для управления процессами чтения-записи данных на магнитных дисках и обмена информацией с шиной данных компьютера.

[12] Энергонезависимая память на флэш-носителях основана на принципе сохранения электрического заряда. В обесточенном состоянии там отсутствуют электрические сигналы. Хотя некоторые специалисты приравнивают сохранение электрического заряда к сохранению дискретного электрического сигнала.

носителей, указывает на теснейшую неотъемлемую взаимосвязь компьютерной информации как предмета преступления и ЭВМ с машинными носителями информации (данных) как орудий совершения преступления. Данный факт позволяет рассматривать компьютерную информацию в ст. 272 и 273 УК РФ в качестве предмета преступления именно как признак объективной стороны преступления.

Третий параграф «Программа для ЭВМ как вид компьютерной информации» посвящён рассмотрению понятия программы для ЭВМ (компьютерной программы), поскольку компьютерная программа как вредоносная упоминается в ст. 273 УК РФ в качестве предмета преступления.

Легальное определение программы для ЭВМ приведено в ст. 1261 Гражданского кодекса (ГК) РФ: «Программой для ЭВМ является представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определённого результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения». Статья 1261 ГК РФ также указывает на то, что программы для ЭВМ (в том числе операционные системы и программные комплексы) могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код.

В диссертации акцентируется внимание на том, что для признания компьютерной информации компьютерной программой важна возможность управляющего воздействия на ЭВМ, а не наличие в составе программы команд и данных, как это предусмотрено ст. 1261 ГК РФ.

Включение законодателем в ст. 1261 ГК РФ в понятие программы для ЭВМ её подготовительных материалов и порождаемых ею аудиовизуальных отображений, очевидно, преследовало цель обеспечения их такой же правовой защитой, как и самих программ. Вместе с тем такое включение нельзя признать удачным, поскольку сами по себе ни подготовительные материалы программ, ни порождаемые ими аудиовизуальные отображения не обладают характеристиками законченных работоспособных программ для ЭВМ. Поэтому подобное расширительное толкование программы для ЭВМ может ввести в заблуждение при применении норм права, не связанных с защитой авторских прав на программы для ЭВМ. Так, подготовительные материалы, полученные в ходе разработки вредоносной программы, а равно порождаемые ею аудиовизуальные отображения, не

способны привести к указанным в ст. 273 УК РФ последствиям вредоносных программ (несанкционированному уничтожению, блокированию, модификации либо копированию информации).

С учётом вышеизложенного предлагается следующее определение компьютерной программы: «Программа для ЭВМ (компьютерная программа) — это данные, предназначенные для управления ЭВМ в целях получения определённого результата. Подготовительные материалы компьютерных программ и порождаемые ими аудиовизуальные отображения охраняются так же, как и компьютерные программы».

В заключение третьего параграфа автор приходит к выводу, что программа для ЭВМ (компьютерная программа), как правило, относится к компьютерной информации, за исключением тех редких случаев, когда она находится на материальных носителях, в форме, не доступной для обработки на ЭВМ (например, в виде записей и изображений на бумаге, доске и т. п.). Вместе с тем компьютерная программа как управляющая ЭВМ компьютерная информация может являться неотъемлемой составной частью ЭВМ, но при этом способна отдельно выступать в качестве предмета преступлений ст. 272 и ст. 273 УК РФ как компьютерная информация.

Вторая глава «Охраняемая законом компьютерная информация» состоит из трех параграфов.

В **первом параграфе «Понятие и виды охраняемой законом компьютерной информации»** указывается на то, что согласно ст. 272 УК РФ предметом преступления является определённая компьютерная информация, которая охраняется конкретным федеральным законом. Поскольку уголовная ответственность предусмотрена за неправомерный доступ к такой информации, то можно сделать вывод, что речь идёт о доступе к информации без соответствующего законного права. Таким образом, конкретный федеральный закон должен ограничивать право доступа к информации определённого содержания, в противном случае нельзя говорить о неправомерном доступе к ней, как, например, о неправомерном доступе к общедоступной информации.

В результате анализа законодательства автор отмечает, что федеральными законами, как правило, ограничивается доступ к информации, прежде всего, для обеспечения её конфиденциальности. В свою очередь, конфиденциальность такой информации защищает интересы (блага) её законного обладателя или иных лиц.

Несмотря на то, что в законах охраняемая информация не упоминается как

компьютерная, это не препятствует признанию её в качестве таковой при обработке посредством ЭВМ или информационной системы. Таким образом, можно констатировать, что охраняемая законом компьютерная информация представлена в составе ст. 272 УК РФ как предмет преступления, который может иметь как экономическую ценность, так и иную значимость для её обладателя.

Автором выделяются обязательные признаки, характеризующие в законе охраняемую от неправомерного доступа информацию, и необязательные (могут отсутствовать в законе), но указывающие на её охрану (факультативные).

К обязательным признакам охраняемой законом информации относятся:

1) описание в федеральном законе содержания такой информации (сведений);

2) указание в федеральном законе на ограничение доступа к такой информации, обеспечение её конфиденциальности, неразглашение, соблюдение (сохранение) в тайне или охрану тайны;

3) административная (по ст. 13.14 КоАП РФ) или уголовная ответственность за её разглашение;

4) обязанность обладателя такой информации или оператора информационной системы, где ведётся её обработка согласно ФЗ «Об информации, информационных технологиях и о защите информации» или соответствующим федеральным законом обеспечить предотвращение несанкционированного доступа к информации и (или) передачи её лицам, не имеющим права на доступ к информации.

Факультативными признаками охраняемой законом информации можно считать:

1) именование в тексте закона тайной или причисление указанных сведений к тайне;

2) указание в тексте закона её обладателей или иных лиц, заинтересованных в обеспечении её охраны;

3) описание в законе или ином нормативном акте порядка доступа к информации;

4) перечисление в законе или ином нормативном акте мер по её защите (охране);

5) предусмотренная законодательством дисциплинарная или гражданская ответственность за незаконные действия с информацией, в том числе нарушение порядка доступа к ней или режима её защиты.

Автор отмечает, что охраняемая законом от неправомерного доступа компьютерная информация ограниченного доступа в случае непринятия её обладателем обязательных

мер по ограничению доступа к ней может быть фактически общедоступной. Так, известны случаи, когда информация, доступ к которой ограничен федеральным законом, была доступна неограниченному кругу посредством сети Интернет. Автор утверждает, что в подобных случаях лицо, получившее доступ к такой компьютерной информации, не подлежит уголовной ответственности, поскольку, во-первых, само по себе обращение лица за информацией к общедоступному ресурсу сети Интернет не нарушает норм права, во-вторых, лицо может не знать о том, что доступ к компьютерной информации, находящейся на этом ресурсе, ограничен законом.

С другой стороны, обладатель информации может предпринимать меры по ограничению доступа к ней, исходя из традиций и/или утратившего силу закона. Подобная ситуация сложилась с 1 января 2008 г. в отношении информации, составляющей служебную тайну, когда утратила силу ст. 139 ГК РФ[13], служившая единственным правовым основанием ограничения доступа к такой информации. При этом на момент отмены ст. 139 ГК РФ федеральный закон о служебной тайне не был принят.

Автор приходит к выводу, что для охраны компьютерной информации от неправомерного доступа большее значение имеют меры по её защите, чем наделение её статусом охраняемой законом. И в уголовно-правовой защите компьютерной информации в первую очередь нуждаются такие её обладатели, которые предприняли реальные меры по обеспечению её безопасности. Информацию ограниченного доступа как предмет преступления ст. 272 УК РФ должно характеризовать именно фактическое ограничение доступа к такой информации, а не только декларируемое законом. Поэтому автор указывает на необходимость внесения соответствующих изменений в ст. 272 УК, в частности фразу «Неправомерный доступ к охраняемой законом компьютерной информации» предлагает заменить на «Неправомерный доступ к компьютерной информации, сопровождающийся нейтрализацией её средств защиты»[14].

Диссертант определяет нейтрализацию средств защиты компьютерной информации как ликвидацию установленных с их помощью ограничений на доступ к компьютерной информации или иное противодействие их функционированию. Приводятся техническое понятие и виды средств защиты компьютерной информации.

---

[13] Гражданский кодекс Российской Федерации. Часть первая от 30 нояб. 1994 г. № 52-ФЗ (в ред. федер. закона Рос. Федерации от 6 дек. 2011 г. № 405-ФЗ) // Собр. законодательства Рос. Федерации. — 1994. — № 32, ст. 3301.

[14] Нейтрализация средств защиты компьютерной информации также упоминается в действующей редакции ст. 273 УК РФ в качестве одного из предназначений вредоносных компьютерных программ.

В заключение второго параграфа предмет преступления, предусмотренный ст. 272 УК РФ, — охраняемую законом компьютерную информацию — автор определяет как компьютерную информацию, доступ к которой должен быть ограничен конкретным федеральным законом и обладателю которой или оператору информационной системы, где ведётся обработка такой компьютерной информации, следует предпринимать необходимые предусмотренные законодательством меры по её защите.

Во **втором параграфе «Неправомерный доступ к охраняемой законом компьютерной информации»** автор указывает на то, что ни одно из нормативных определений не учитывает специфику доступа именно к компьютерной информации посредством ЭВМ. Под доступом к компьютерной информации он предлагает понимать возможность её уничтожения, блокирования, модификации или копирования с помощью ЭВМ. То есть доступ к ЭВМ, обеспечивающий только ознакомление с обрабатываемой на ней информацией нельзя признать доступом к компьютерной информации.

Отмечается, что понятие неправомерного доступа нормативно не определено. Вместе с тем существует близкое по значению к неправомерному доступу понятие несанкционированного доступа к компьютерной информации, определение которого приведено в Руководящем документе Гостехкомиссии России. «Защита от несанкционированного доступа к информации. Термины и определения». Согласно п. 4 указанного документа, «несанкционированный доступ к информации (НСД), то есть доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем»[15].

Ограничение доступа к информации также предполагает определённый порядок реализации такого ограничения (доступа к информации), который может быть предусмотрен как в самом законе, так и в подзаконных нормативных актах. Отсутствие такого порядка вынуждает апеллировать к лицу, в чьих интересах закон охраняет

[15] Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения (утв. решением Государственной технической комиссии при Президенте РФ от 30 марта 1992 г.) // Сайт Федеральной службы по техническому и экспортному контролю. URL: http://www.fstec.ru/index.php/ru/component/content/article/114-deyatelnost/tekushchaya/tekhnicheskaya-zashchita-informatsii/normativnye-i-metodicheskie-dokumenty/spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3 (дата обращения: 08.02.2013).

конфиденциальность определённой информации — её обладателю[16], точнее к наличию санкции (разрешения) на доступ к информации.

Таким образом, автор приходит к выводу, что неправомерным будет являться доступ к охраняемой законом компьютерной информации, совершенный (совершаемый) либо в нарушение нормативно предусмотренного порядка доступа к ней, либо (в случае, когда порядок доступа к компьютерной информации не установлен) при отсутствии разрешения на доступ со стороны её обладателя или его законного представителя.

Особо отмечается, что уголовная ответственность по ст. 272 УК РФ наступает в случае неправомерного доступа к компьютерной информации, но не в случае совершения неправомерных действий с компьютерной информацией лицами, имеющими права доступа к ней. Такого рода деяния по каким-то причинам не нашли своего отражения среди преступлений в сфере компьютерной информации УК РФ, хотя были предусмотрены в модельном УК для государств-участников СНГ 1996 г.[17]

Третий параграф «Общественно опасные последствия неправомерного доступа к охраняемой законом компьютерной информации» посвящён определению не нашедших отражения в законодательстве понятий блокирования, модификации, уничтожения и копирования компьютерной информации.

Под блокированием компьютерной информации автор предлагает понимать прекращение доступа пользователей ЭВМ к компьютерной информации, не связанное с её уничтожением и не являющееся результатом функционирования средств защиты компьютерной информации.

Отмечается, что уничтожение можно считать одним из самых опасных последствий действий с компьютерной информацией, поскольку оно заключается в её утрате. Причём зачастую применительно к компьютерной информации уничтожение и удаление употребляются как синонимы. Однако автор указывает на различие этих понятий. Так, при удалении файлов или каталогов с использованием штатного программного обеспечения операционной системы семейства Microsoft Windows происходит лишь объявление конкретного места на логическом диске свободным от удалённых файлов или каталогов,

[16] Обладатель информации — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам (п. 5 ст. 2 ФЗ «Об информации, информационных технологиях и о защите информации» 2006 г.).
[17] Модельный Уголовный кодекс для государств - участников СНГ (принят постановлением Межпарламентской Ассамблеи государств - участников СНГ от 17 февраля 1996 г.). Информационный бюллетень Межпарламентской Ассамблеи государств - участников СНГ, 1997 г., № 10.

хотя их информация ещё там присутствует. Стираться информация удалённых файлов или каталогов будет лишь при записи на это же место новой информации. Поэтому существует возможность восстановления удалённой, но не окончательно стёртой компьютерной информации специальными компьютерными программами. Но, удаление компьютерной информации представляет реальную угрозу её утраты, поскольку создаются условия для записи новой компьютерной информации на месте удалённой. Удаление компьютерной информации при возможности восстановления может быть признано её блокированием, поскольку доступ к удалённой информации с использованием штатных программных средств ЭВМ, как правило, невозможен до тех пор, пока она не будет восстановлена.

Изучив теорию и практику восстановления компьютерной информации, автор считает, что признание факта уничтожения компьютерной информации будет зависеть от применяемых технологий её восстановления в каждом конкретном случае. Данное обстоятельство может представлять проблему для квалификации деяний по ст. 272 и 273 УК РФ. Поэтому в определении уничтожения компьютерной информации автор счёл необходимым указать на ограничение возможности её восстановления только программными методами. В итоге уничтожение компьютерной информации он определил как действия над ней, приводящие к её утрате при невозможности восстановления программными средствами ЭВМ.

Под модификацией компьютерной информации автор предлагает понимать внесение любых изменений на логическом уровне её представления (в секторе, сетевом пакете, файле, каталоге, логическом диске).

Под копированием компьютерной информации он понимает процесс её переноса с использованием средств ЭВМ с одного носителя на другой без изменения количества и качества, при котором она сохраняется на исходном носителе. При этом отмечается, что создание бумажной копии может быть также признано копированием компьютерной информации, поскольку информация выводится (распечатывается) на бумаге с использованием компьютера и принтера[18] (средств ЭВМ).

Автор обращает внимание на тот факт, что такое общественно опасное последствие неправомерного доступа к компьютерной информации, как «нарушение работы ЭВМ, системы ЭВМ или их сети», исключено законодателем из состава ст. 272 УК РФ. Также оно исключено из ст. 273 УК РФ как последствие использования вредоносной

[18] Принтер относится к устройствам вывода информации ЭВМ.

компьютерной информации. Он полагает, что нарушение работы ЭВМ, системы ЭВМ или их сети может проявляться без признаков уничтожения, блокирования, модификации или копирования компьютерной информации пользователя, но представлять собой не меньшую общественную опасность. Автор считает неоправданным исключение из ст. 272 и 273 УК РФ нарушения работы ЭВМ, систем ЭВМ или их сетей как последствия неправомерного доступа или использования вредоносной компьютерной информации.

В заключение третьего параграфа автор приходит к выводу, что опасное воздействие на компьютерную информацию далеко не всегда характеризуется процессами её удаления, модификации, блокирования или копирования, поскольку эти процессы присущи штатной работе любой ЭВМ. Вместе с тем формы вредного умышленного воздействия на компьютерную информацию целесообразно криминализовать в виде компьютерного саботажа — умышленного уничтожения или повреждения компьютерной информации либо нарушения работы или выведения из строя ЭВМ, информационных систем или информационно-телекоммуникационных сетей.

Третья глава «Вредоносная компьютерная информация» состоит из трёх параграфов.

В **первом параграфе «Понятие вредоносной компьютерной информации»** автор акцентирует внимание на том, что в новой редакции ст. 273 УК РФ к вредоносным отнесены не только компьютерные программы, но и иная компьютерная информация, так же как и программы, заведомо предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. Поэтому в названии статьи правильнее использовать термин «вредоносная компьютерная информация» вместо «вредоносные компьютерные программы». Расширив предмет преступления ст. 273 УК РФ, законодатель тем самым позволил правоприменителю не проводить оценку компьютерной информации на предмет её отношения к программам для ЭВМ в соответствии со ст. 1261 ГК РФ, недостатки которой мы рассматривали выше.

Между тем автор указывает на то, что могут иметь место отдельные команды или данные (не организованные в соответствии с алгоритмом как программы), приводящие к вредным последствиям. Например, возможность нарушения работы ЭВМ (программы для ЭВМ) может повлечь ввод команд или данных, неверно воспринятых ЭВМ (программой ЭВМ).

В ходе изучения способов опасного автоматизированного воздействия на компьютерную информацию, ЭВМ, информационные системы и информационно-телекоммуникационные сети, а также в результате анализа баз данных антивирусных средств защиты автор пришёл к выводу, что вредоносная компьютерная информация в большей степени представлена именно компьютерными программами.

Отмечается, что вред пользователю ЭВМ способны причинить не только так называемые вредоносные, но и полезные программы. Причинами наступления вредных последствий выполнения на ЭВМ полезных программ, как правило, являются:

1) неквалифицированные действия пользователей;
2) злонамеренное использование потенциально опасных функций программ;
3) конфликты между программами;
4) ошибки, допущенные при создании программ.

При этом практически во всех лицензионных соглашениях на использование программ для ЭВМ указано, что их создатели не несут ответственности за вред, причинённый программой, тем самым признавая потенциальную опасность своих программных продуктов. Вместе с тем с учётом повсеместной автоматизации, программный сбой ЭВМ может повлечь достаточно тяжелые последствия и большие убытки.

Автор отмечает, что в новой редакции ст. 273 УК РФ к вредоносным сейчас причислены компьютерные программы и иная компьютерная информация, не только заведомо предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования, но и для нейтрализации средств защиты компьютерной информации. Последствия выполнения вредоносной программы или обработки вредоносной компьютерной информации, указанные в ст. 273 УК РФ, схожи с последствиями неправомерного доступа уже рассмотренной выше ст. 272 УК РФ (кроме нейтрализации средств защиты компьютерной информации).

Автором подчёркивается, что понятие нейтрализации средств защиты компьютерной информации характеризует действия лица, осуществляющего неправомерный доступ к ней, но не действия законного обладателя такой информации со средствами её защиты. Поэтому она не может быть санкционированной. Следовательно, в диспозиции ст. 273 УК РФ «несанкционированного» не следует распространять на нейтрализацию средств защиты компьютерной информации.

Под несанкционированным уничтожением, блокированием, модификацией, копированием информации некоторые юристы предлагают понимать не разрешённые законом, обладателем информации или другим компетентным пользователем указанные действия[19]. Соискатель обращает внимание, что тем самым несанкционированный характер действий программы с компьютерной информацией увязывается с её обладателем. Однако выявить обладателя информации на этапах создания, изменения или распространения вредоносной компьютерной программы весьма затруднительно. Автор считает, что в таких ситуациях установить несанкционированный характер действия программы можно только относительно потенциального потерпевшего — пользователя (оператора) ЭВМ или информационной системы, на которой наступят вредные последствия работы такой программы.

Диссертант отмечает, что практически все компьютерные программы имеют функции модификации, удаления, копирования информации, выполняемые автоматически, без ведома и разрешения пользователя ЭВМ, то есть фактически несанкционированно. Но на этом основании относить их к вредоносным было бы неправильно, поскольку целью автоматизации процессов с помощью ЭВМ является как раз освобождение человека (пользователя ЭВМ) от рутинных операций. Насколько необходимо посвящать пользователя компьютерной программы в суть выполняемых ею функций, решают создатели программы в зависимости от её назначения и предполагаемой квалификации пользователя. Для вредоносных программ, по мнению автора, кроме несанкционированного действия, характерно вредоносное (опасное) назначение.

В заключение первого параграфа соискатель делает вывод о том, что несанкционированное уничтожение, блокирование, модификация или копирование компьютерной информации далеко не всегда можно признать общественно опасными последствиями или назначением вредоносной компьютерной информации. Таковыми следует считать значительный ущерб и (или) существенный вред правам и законным интересам граждан или организаций либо охраняемым законом интересам общества или государства.

Второй параграф **«Виды вредоносной компьютерной информации»** посвящён анализу существующих разновидностей опасных компьютерных программ и иной

[19] Комментарий к Уголовному кодексу Российской Федерации. Изд. 2-е, изм. и доп./ Под общ. ред. проф. Ю.И. Скуратова В.М. Лебедева.— М.: НОРМА — ИНФРА-М, 1999. С. 641.

компьютерной информации на предмет возможности отнесения их к числу вредоносных.

Рассматриваются существующие классификации опасных программ антивирусных лабораторий (организаций) и независимых исследователей. Отмечается, что основания данных классификаций зачастую отражают лишь их функциональные возможности без учёта признаков вредоносной компьютерной информации, приведённых в ст. 273 УК РФ. Вместе с тем указанные классификации способствуют выделению характерных видов и адекватной оценке степени опасности компьютерной информации.

Автор критикует точки зрения юристов на вредоносные компьютерные программы. В частности, широко распространено мнение, что компьютерные вирусы являются вредоносными программами. Зачастую эти два понятия употребляются как синонимы. Однако соискатель подчёркивает, что изначально основным признаком компьютерного вируса является его способность к самораспространению (саморазмножению). И саморазмножение компьютерного вируса нельзя, по мнению диссертанта, относить к несанкционированному копированию компьютерной информации пользователя ЭВМ, поскольку при этом отсутствует характерная для несанкционированного копирования угроза нарушения конфиденциальности компьютерной информации. Поэтому компьютерный вирус как таковой нельзя автоматически относить к вредоносным программам. Он может быть признан вредоносной программой, только если процесс его саморазмножения негативно воздействует на работу ЭВМ или на компьютерную информацию её пользователя.

В результате сопоставления существующих видов опасных компьютерных программ с признаками вредоносной компьютерной информации ст. 273 УК РФ соискатель выделяет виды вредоносных компьютерных программ. Вместе с тем он отмечает существование компьютерных программ, не имеющих признаков вредоносных, но предназначенных для причинения вреда пользователям ЭВМ и/или нарушения их прав. Данный факт, по мнению диссертанта, свидетельствует о недостатках конструкции состава ст. 273 УК РФ.

Автор, основываясь на анализе существующих видов общественно опасной компьютерной информации и передового зарубежного опыта криминализации действий с ней, предлагает под вредоносной компьютерной информацией в УК РФ понимать компьютерные программы или иную компьютерную информацию, предназначенные для воздействия на ЭВМ, информационную систему или информационно-

телекоммуникационную сеть вопреки интересам их пользователей или владельцев, а равно в целях причинения вреда им или иным лицам.

В заключение параграфа соискатель отмечает, что для получения доступа к компьютерной информации в ходе оперативно-розыскной деятельности, при производстве по делу об административном нарушении, при производстве дознания, предварительного следствия или осуществлении правосудия могут использоваться специальные компьютерные программы или иная компьютерная информация, которые формально могут иметь признаки вредоносных программ, например, программы для скрытого копирования информации с компьютера подозреваемого или программы (или иная компьютерная информация) для нейтрализации средств защиты компьютерной информации. Без использования таких программ раскрытие преступлений, сопряжённых с использованием ЭВМ, по сути, невозможно. Поэтому диссертант считает необходимым в ст. 273 УК РФ отдельно указать, что компьютерные программы и иная компьютерная информация, предназначенные для использования или использующиеся в правоохранительных целях, не относятся к вредоносным при условии их использования лицами, наделёнными соответствующими полномочиями.

В третьем параграфе **«Преступные деяния с вредоносной компьютерной информацией»** раскрывается содержание понятий создания, использования и распространения вредоносных компьютерных программ иной компьютерной информации.

Автор отмечает, что законами определены понятия «распространение информации»[20] и «использование произведения»[21], к произведениям в соответствии со ст. 1225 и 1261 ГК РФ относятся программы для ЭВМ. Определение понятий создания компьютерной программы или иной компьютерной информации не приводится ни в одном нормативном правовом акте.

Диссертант предлагает понимать в ст. 273 УК РФ под созданием вредоносной компьютерной информации действия, направленные на её создание, в том числе внесение изменений в существующую компьютерную информацию с целью получения вредоносной компьютерной информации.

---

[20] П 9 ст. 2 ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 152-ФЗ (в ред. федер. закона Рос. Федерации от 28 июля 2012 г. № 139-ФЗ) // Собр. законодательства Рос. Федерации. — 2006. — № 31, ч. 1, ст. 3448 (далее — ФЗ «Об информации, информационных технологиях и о защите информации»).
[21] Ст. 1270 ГК РФ. Гражданский кодекс Российской Федерации. Часть четвертая от 18 дек. 2006 г. № 230-ФЗ (в ред. федер. закона Рос. Федерации от 8 дек. 2011 г. № 422-ФЗ) // Собр. законодательства Рос. Федерации. — 2006. — № 52, ч. 1, ст. 5496.

Указывается, что передача вредоносной компьютерной информации как определённым лицам (предоставление информации[22]), так и неопределенному кругу лиц (распространение информации) представляет общественную опасность. Таким образом, по мнению соискателя, понятие «распространение вредоносной компьютерной информации» должно быть шире, чем приведённое в ФЗ «Об информации, информационных технологиях и о защите информации» понятие «распространение информации». Поэтому он считает, что под распространением вредоносной программы или иной компьютерной информации при квалификации деяния по ст. 273 УК РФ следует понимать действия, направленные на её передачу или предоставление доступа к ней любому лицу.

Диссертант отмечает, что вредоносную компьютерную информацию, очевидно, необходимо рассматривать через призму признаков компьютерной информации, приведённых в приложении 1 к ст. 272 УК РФ, а именно как представленную в виде электрических сигналов. Но, как он указывал выше, электрические сигналы отсутствуют на оптических дисках, в обесточенных НЖМД, флэш-носителях, в радиоканале и в оптоволоконном кабеле, что указывает на невозможность присутствия там вредоносной компьютерной информации. Таким образом, по мнению автора, последние редакции ст. 272 и 273 фактически декриминализируют распространение вредоносных программ и иной компьютерной информации на машинных носителях. Хотя в предыдущей редакции ст. 273 УК РФ отдельно указывалось на распространение машинных носителей с такими программами[23]. Соискатель не находит оснований для исключения уголовной ответственности за такую форму распространения вредоносной компьютерной информации.

Согласно п. 2 ст. 1270 ГК РФ использование программы для ЭВМ включает в себя понятия распространения и воспроизведения программы для ЭВМ. Автор отмечает, что «распространение» отдельно упоминается в ст. 273 УК РФ. Кроме того, в формулировке понятия «воспроизведение» как составной части понятия «использование», приведённого в ГК РФ, ничего не сказано о выполнении программы для ЭВМ, а упоминается лишь «запись в память ЭВМ». Поскольку запись в память ЭВМ не гарантирует запуск программы на выполнение, то и использование вредоносной программы в трактовке ГК

[22] П. 8 ст. 2 ФЗ «Об информации, информационных технологиях и о защите информации».
[23] Многие юристы, в том числе и автор, считают, что упоминание распространения машинных носителей с вредоносными программами в предыдущей редакции ст. 273 УК РФ было излишне, поскольку оно является всего лишь одним из способов уже предусмотренного ст. 273 УК РФ распространения вредоносных программ.

РФ не гарантирует наступление названных в диспозиции ст. 273 УК РФ последствий. Тем самым автор снова указывает на несостоятельность использования норм ГК РФ для толкования ст. 273 УК РФ.

По мнению соискателя, использование вредоносной компьютерной программы по смыслу ст. 273 УК РФ следует понимать как применение её по назначению. Использование иной вредоносной компьютерной информации, не относящейся к компьютерной программе, возможно путём её ввода в память ЭВМ, однако это не всегда гарантирует наступление вредных последствий.

В заключение третьего параграфа автор под использованием вредоносной компьютерной информации предлагает понимать применение такой информации по назначению, а равно запуск на выполнение компьютерной программы на ЭВМ или подготовка её к неизбежному запуску на выполнение.

В **заключении** изложены основные выводы диссертационного исследования и даны сформулированные автором предложения по внесению изменений в законодательство.

Основные положения диссертационного исследования опубликованы в следующих работах автора:

В ведущих рецензируемых научных изданиях, указанных в перечне ВАК

1. Челноков В.В. О вредоносности программ для ЭВМ // Сборник трудов Института ФСБ России (г. Екатеринбург). 2008. С. 59-63 (0,3 п.л.).
2. Челноков В.В. О правомерности ограничения доступа или распространения сведений «Для служебного пользования» // Сборник трудов Института ФСБ России (г. Екатеринбург). 2008. С. 63-66 (0,2 п.л.).
3. Челноков В.В. О роли ФСБ России в противодействии вредоносным программам // Специальный сборник ФСБ России. 2010. № 223 (291). С. 49-53 (0,4 п.л.).
4. Челноков В.В. Уголовно-правовая оценка несанкционированного использования вычислительных ресурсов // Уголовное право. Научно-практический журнал. 2010. № 4. С. 69-72 (0,4 п.л.).

В иных изданиях

5. Челноков В.В. Квалификация создания, использования и распространения вредоносных программ для ЭВМ // Материалы региональной научно-практической конференции на специальную тему. — Новосибирск: ИППКС ФСБ России. 2001, с. 120 – 124. (0,3 п.л.).
6. Челноков В.В. Правовая оценка наличия информации о гражданах в базах данных // Информационная безопасность региона: сборник научных трудов I Всероссийской научно-практической конференции 5-7 октября 2004 г./ Науч. ред. Ю.Т. Карманов, Л.В. Астахова. — Челябинск: Изд-во ЮУрГУ. 2005. С. 119-121 (0,1 п.л.).
7. Челноков В.В. Программы для ЭВМ, представляющие опасность, и квалификация действий с ними // Уголовная политика в сфере информационной безопасности Российской Федерации: материалы IV Международной научно-практической конференции, посвященной памяти М. И. Ковалева (Екатеринбург, 10 февраля 2007 г.). — Екатеринбург : УрГЮА, 2007. С. 198-204 (0,3 п.л.).
8. Челноков В.В. Криминалистические аспекты последних изменений составов преступлений в сфере компьютерной информации // Актуальные проблемы теории и практики компьютерной криминалистики: материалы ведомственной научно-практической конференции — Екатеринбург: Институт ФСБ России. 2012. С. 210 – 212 (0,1 п.л.).