LEGAL REGULATION OF THE PROTECTION OF INTELLEKTUAL RIGHTS OF MINORS

***E.A. Dzhalilov*,** candidate of law sciences, associate professor of «Business and labor law»
E.A. Dzhalilova, candidate of law sciences, associate professor of «Business and labor law»
Togliatti State University, Togliatti (Russia)

Annotation: The legal status of minors in the area of intellectual property rights, identify problems existing legislation in this area.

Keywords: intellectual property, copyrights, patent rights, the legal status of minors.

УДК 343.2/.7

ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОЙ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

***К.Н. Евдокимов*,** кандидат юридических наук, доцент, доцент кафедры государственно-правовых дисциплин
Иркутский юридический институт (филиал) Академии Генеральной прокуратуры РФ, Иркутск (Россия)

Аннотация: Статья посвящена вопросам уголовно-правовой квалификации преступлений в сфере компьютерной информации. Автор проводит анализ наиболее актуальных проблем, с которыми сталкивается правоприменитель при квалификации преступных деяний данного вида и вносит предложения по совершенствованию действующего уголовного законодательства.

Ключевые слова: компьютерная преступность, преступления в сфере компьютерной информации, неправомерный доступ к компьютерной информации, программы для ЭВМ, вредоносные компьютерные программы.

В Российской Федерации за последние годы наметилась тенденция к качественной трансформации содержания и сущности компьютерной преступности, что нашло выражение в приобретении последней все более транснационального, организованного, экономического и политического характера. При этом вред, причиняемый российскому обществу и экономике, преступлениями в сфере компьютерной информации носит колоссальный характер.

Так, по оценкам аналитиков компании Group-IB объем рынка киберпреступности в РФ в 2012 году составил 1,93 миллиарда долларов [1].

В свою очередь, американская корпорация Symantec оценила ущерб от киберпреступности в России за 2013 год в 1 миллиард долларов, а в 2012 году в 1,48 миллиарда долларов. При этом общий ущерб от киберпреступности в мире в 2013 году составил 113 миллиардов долларов, против 110 миллиардов долларов в 2012 году [2].

Одной из проблем противодействия компьютерной преступности является правильная уголовно-правовая квалификация преступлений в сфере компьютерной информации на стадии предварительного следствия. Поскольку, безошибочная юридическая квалификация преступления определяет выбор следователем (судьей) меры пресечения обвиняемому и наказания для подсудимого, предопределяет форму расследования и подсудность уголовного дела.

Однако при квалификации преступлений в сфере компьютерной информации правоприменитель часто сталкивается с затруднениями юридического характера.

Так, например, у следователя или судьи возникает проблема при уяснении некоторых понятий, содержащихся в диспозициях ст.ст.272-274 УК РФ, а именно: «компьютерная программа», «несанкционированное уничтожение, блокирование, модификация, копирование компьютерной информации», «нейтрализация средств защиты компьютерной информации», «средства хранения, обработки или передачи охраняемой компьютерной информации». Это связано с тем, что указанные юридические термины законодательно нигде не определены. В этих случаях судья, прокурор, следователь вынуждены обращаться к текстам комментариев к Уголовному кодексу РФ, где данные понятия разъясняются научными и практическими работниками. Однако при этом, в отсутствие разъяснений пленума Верховного Суда РФ, выводы авторов носят субъективный, а иногда и взаимопротиворечивый характер. Что, к сожалению, негативно влияет на единообразие судебно-следственной практики по рассмотрению и расследованию преступлений в сфере компьютерной информации.

Кроме того, при квалификации деяний, предусмотренных ст. ст. 272-274 УК РФ возникает ряд вопросов, требующих толкования для правоприменителя.

Например, будет ли являться уничтожением компьютерной информации, деяние при котором информация была изначально уничтожена, но спустя определенное время частично или полностью восстановленная специалистами? Как квалифицировать уничтожение компьютерной информации сильным электромагнитным или высокочастотным излучением, не повлекшим уничтожение самого носителя информации? Будет ли являться копированием компьютерной информации действия преступника при получении копии путем распечатывания информации на принтере, фотографирования или видеосъемки изображения с монитора компьютера?

Наконец, как квалифицировать несанкционированное ознакомление с компьютерной информацией, когда преступник, визуально запомнив конфиденциальные сведения (например, персональные данные лица; информацию о содержании коммерческой сделки и сторонах договора; сведения об усыновлении (удочерении), врачебную тайну и т.д.), впоследствии переносит их на другой материальный носитель информации, создав ее копию (написав на листе бумаги, введя информацию в память своего компьютера или иного компьютерного устройства: айфона, смартфона, планшетного компьютера, коммуникатора и т.п.).

По нашему мнению, описанные случаи содержат признаки неправомерного уничтожения или копирования компьютерной информации.

Автор согласен с проф. С.В. Бородиным, что способы неправомерного доступа к компьютерной информации могут быть самыми различными, например, представление фиктивных документов на право доступа к информации, изменение кода или адреса технического устройства, нарушение средств или системы защиты

информации, кража носителя информации [3, с.664].

Однако полагаем целесообразным дополнить главу №28 УК РФ статьей 272.1: «Статья 272.1 Незаконное завладение носителем компьютерной информации с целью осуществления неправомерного доступа к компьютерной информации». Данная авторская позиция обусловлена тем, что преступник тайно, открыто или обманным путем завладев, например, флэш-картой или DVD-диском с компьютерной информацией для последующего ее использования, избегает уголовной ответственности в силу малозначительности совершенного деяния, т.к. стоимость вышеуказанных носителей информации не превышает тысячи рублей, что влечет для правонарушителя, в лучшем случае, наступление административной ответственности по ст.7.27 КоАП РФ (мелкое хищение) и наказание до 15 суток административного ареста. При этом виновное лицо получает доступ к компьютерной информации, которая представляет большую ценность для ее владельца, чем сам материальный носитель информации.

При квалификации преступных действий, предусмотренных ст.273 УК РФ, следует отметить неудачную с точки зрения законодательной техники юридическую конструкцию ч.1 ст.273 УК РФ, в диспозиции которой указывается на «создание, распространение или использование компьютерных программ … заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации». Указание законодателем на создание, использование и распространение вредоносных компьютерных программ во множественном числе, по смыслу статьи можно трактовать как то, что правоприменитель не вправе привлекать к уголовной ответственности лицо, которое создало, использовало или распространило одну вредоносную компьютерную программу.

Поэтому автор согласен с проф. В.С. Комиссаровым, который высказал мнение, что «…смысл уголовной ответственности за данное преступление определяется не столько количественными факторами, сколько потенциально вредоносным качеством конкретной программы, в частности ее способностью причинить реальный общественно опасный вред информации и деятельности ЭВМ. Поэтому применение ст. 273 возможно уже в случаях создания, использования и распространения одной вредоносной программы для ЭВМ или одного машинного носителя с такой программой» [4, с.533].

Вышеуказанный недостаток законодательства вполне может быть устранен соответствующим постановлением пленума Верховного Суда РФ.

Также, по мнению автора, нецелесообразным является исключение из диспозиции ст.273 УК РФ такого преступного действия как «внесение изменений в существующие программы». Данный вопрос приобретает актуальность в связи с тем, что в последние годы создаются, используются и распространяются уже не отдельные вредоносные программы, а целые семейства компьютерных вирусов, имеющих однотипную компьютерную программу или компьютерный код.

Так, например, вирусмейкеры Джеффри Ли Парсон (США) и Димитрий Чобан (Румыния) модифицировали компьютерный вирус «Blaster», который нанес в 2003-2005 годах ущерб от 2 до10 млрд. долларов владельцам и пользователям компьютеров в США и странах Европы. Однако по их признанию, они не создавали вредоносную компьютерную программу «Blaster», а произвели ее модификацию, т.е. внесли изменение в существующую вредоносную компьютерную программу, получив тем самым компьютерные вирусы «Blaster.B» и «Blaster.F» [5].

Думается, что с уголовно-правовой точки зрения, постановление пленума Верховного Суда РФ могло бы устранить сомнения в части, считать ли подобные действия модификацией, т.е. внесением изменений в существующую вредоносную компьютерную программу (информацию), либо созданием новой вредоносной компьютерной программы (информации).

По нашему мнению, в данном случае, виновное лицо должно нести ответственность в равной степени, как за модификацию, так и за создание своей разновидности вредоносной программы.

Кроме того, считаем логичным в число преступных действий, закрепленных в ч.1 ст.273 УК РФ включить такое деяние как приобретение компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Свою позицию обосновываем тем фактом, что подавляющее большинство преступников использующих вредоносные компьютерные программы не являются их создателями, а приобретают их для преступных целей у представителей хакерского сообщества, на хакерских сайтах и веб-страницах, а также путем обмена через электронные доски объявлений или хакерские форумы. При этом вредоносные компьютерные программы, также как и оружие, наркотики, сильнодействующие или психотропные вещества, взрывчатые вещества наносят существенный вред обществу. Поэтому лица, приобретающие компьютерные вирусы, должны нести уголовную ответственность наравне с лицами их создающими и распространяющими.

Данная точка зрения уже высказывалась ранее рядом авторов [6, с.98; 7, с.86], но законодательного закрепления не нашла.

Вызывает определенное недоумение также установление законодателем в ч.2 ст. ст. 272, 273, ч.1 ст.274 УК РФ уголовной ответственности за причинение крупного ущерба, сумма которого превышает один миллион рублей.

При этом, например, размер крупного ущерба в ч.ч.1,2 ст.146 за причинение вреда авторским или смежным правам установлен в сто тысяч рублей, а за преступления против собственности (ст.ст.158,159, 163, 167 УК РФ) в размере превышающим двести пятьдесят тысяч рублей. Таким образом, по мнению автора, размер крупного ущерба при совершении преступлений в сфере компьютерной информации явно завышен, что также негативно влияет на уголовно-правовую квалификацию преступных деяний указанного вида.

Как следствие, немалое количество компьютерных преступников получило возможность избежать уголовной ответственность в силу того, что причиненный ими вред ниже установленного законодателем размера нанесенного ущерба, а количество уголовных дел, возбужденных по преступлениям в сфере компьютерной информации значительно сократилось. Так, согласно данным ГИАЦ МВД России было зарегистрировано преступлений, предусмотренных ст. ст. 272, 273, 274 УК РФ: в 2010 г. – 6132, 1010, 0 [8], в 2011 г. – 2005, 693, 0 [9], в 2012 г. – 1930, 889, 1[10], в 2013 г. – 1799, 764.

Кроме того, компьютерная информация, технические средства ее обработки, носители информации могут находиться в собственности физических лиц. Поэтому, по нашему мнению, представляется целесообразным учесть имущественные права и интересы потерпевшего, дополнив диспозицию ст. ст. 272, 273 УК РФ новым квалифицирующим признаком: «с причинением значительного ущерба гражданину...».

С учетом вышесказанного, считаем целесообразным снизить крупный размер вреда, причиненного преступлением в сфере компьютерной информации и изложить примечание к ст.272 УК РФ в следующей редакции: «1. Под компьютерной информацией

понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

2. Значительный ущерб гражданину в статьях настоящей главы определяется с учетом его имущественного положения, но не может составлять менее двух тысяч пятисот рублей.

3. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает сто тысяч рублей».

Это позволит привести ст.ст.272-274 УК РФ в соответствие с остальными уголовно-правовыми нормами по вопросу о размере ущерба, причиненного преступным деянием, устранив в данном случае возникшую диспропорцию в размерах причиненного вреда.

Продолжая анализ проблем квалификации преступлений в сфере компьютерной информации, нельзя не остановиться на мотивах и целях преступления.

Необходимо отметить, что в действующей редакции ч.3 ст.272 УК РФ и ч.2 ст.273 УК РФ в качестве квалифицирующего признака преступления закреплен корыстный мотив: «Деяния, … совершенные из корыстной заинтересованности». Это положительный шаг в совершенствовании уголовной ответственности за преступные деяния данного вида, т.к. по мнению большинства опрошенных работников правоохранительных органов (74 %), корыстный мотив присутствует не менее чем в 90 % случаев совершения преступлений в сфере компьютерной информации [11, с.27].

Однако считаем целесообразным, дополнить диспозицию статей 272, 273 УК РФ новым квалифицирующим признаком: «С целью скрыть другое преступление или облегчить его совершение», поскольку преступления в сфере компьютерной информации часто выступают способом совершения множества других преступных деяний (хищения чужого имущества, умышленного уничтожения или повреждения имущества, шпионажа, государственной измены и т.д.).

Анализ научных трудов, посвященных совершенствованию уголовной ответственности за преступления в сфере компьютерной информации, подтверждает позицию автора об учете вышеуказанной целей для всесторонней и полной квалификации рассматриваемых преступных деяний.

Так, М.М. Менжега указывает, что целями использования и распространения вредоносных программ, помимо несанкционированного уничтожения, блокирования, модификации или копирования информации, могут быть стремление совершить иное преступление, либо скрыть следы уже совершенного [12, с.58].

Аналогичной позиции придерживается М.М. Малыковцев считающий, что если виновный преследует цель совершить с помощью использования и распространения вредоносной программы иное преступление, то мотив и цель могут быть и обязательными признаками преступления [13, с.115-116].

Нельзя не учитывать и политические мотивы (цели) совершения преступлений в сфере компьютерной информации, которые, по мнению автора, вызваны: 1) развитием хактивистского движения как политического протестного движения против государственного контроля в глобальной информационной сети «Интернет» и нарушения информационных прав человека; 2) причинением вреда государственным интересам, деятельности механизма государственной власти Российской Федерации вооруженными силами враждебных стран, путем использования вредоносных компьютерных программ в качестве информационного оружия; 3) деятельностью спецслужб иностранных государств в отношении российских органов власти, учреждений, предприятий для получения информации геополитического, военно-технического, дипломатического и иного стратегического характера, т.е. «кибершпионаж», 4) неправомерным использованием вредоносных компьютерных программ и компьютерных технологий в период предвыборных компаний для дискредитации кандидатов на выборные должности в органы государственной власти и местного самоуправления.

Поэтому для более эффективного противодействия преступлениям в сфере компьютерной информации автор предлагает дополнить диспозиции ч.3 ст.272, ч.2 ст.273, ч.1 ст.274 УК РФ новым квалифицирующим признаком: «Те же деяния, совершенные с целью устрашения населения или воздействия на принятие решения органами государственной власти и (или) местного самоуправления, а также воспрепятствования нормальной деятельности средств массовой информации, органов государственной власти и местного самоуправления, государственных и муниципальных учреждений, предприятий», установив санкцию до 10 лет лишения свободы.

При этом, автор полагает, необходимым внести изменения в ст.151 УПК РФ и отнести преступления, предусмотренные ч.ч.2,3,4 ст.272, ч.ч.2,3 ст. 273, ч.ч.1,2 ст.274 УК РФ к подследственности органов ФСБ РФ.

Также, по мнению автора, пробелом отечественного уголовного законодательства является отсутствие нормы об уголовной ответственности юридических лиц, в т.ч. за компьютерные преступления.

В частности, 23 ноября 2001 г. в Будапеште была принята Конвенция о киберпреступности [14], ратифицированная 47-ю государствами. К сожалению, Россия не является страной-участницей данной Конвенции как раз по причине отсутствия в УК РФ нормы, предусматривающей уголовную ответственность юридических лиц. Это, безусловно, создает препятствия эффективному международному сотрудничеству в борьбе с компьютерной преступностью.

Дискуссия о необходимости введения в российское законодательство института уголовной ответственности юридических лиц ведется уже несколько десятилетий и автор поддерживает тех ученых [15, с.214-215; 16, с.243; 17, с.195; 4, с.280-284], которые считают, что закрепление уголовно-правовой нормы об ответственности юридических лиц, расширило бы правовой инструментарий противодействия российской преступности. В свою очередь, правовая регламентация уголовной ответственности юридических лиц за совершение компьютерных преступлений в зарубежном законодательстве (Австралия, Албания, Бельгия, Великобритания, Венгрия, Дания, Израиль, Индия, Ирландия, Исландия, Канада, КНР, США, Франция и др.) доказывает практическую целесообразность данного шага.

СПИСОК ЛИТЕРАТУРЫ

1. URL: http://digit.ru/business/20130910/405335397.html#ixzz2r1xUjpbf (Дата обращения 07.10.2014).

2. URL: http://go.symantec.com/norton-report-2013/ (Дата обращения 07.10.2014).

3. Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. доктор юридических наук, профессор А.В. Наумов. – М.: Юристъ, 1996. – 824 с. (Автор главы - доктор юридических наук, профессор С.В. Бородин)

4. Уголовное право: особенная часть / под ред. А.И. Рарога. – М.: Эксмо, 2009. – 704 с.

5. URL: http://ru.wikipedia.org/wiki/Blaster_%28%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D%80D0%BD%D1%8B% D0%B9 %D1%87%D0%B5%D1

%80%D0%B2%D1%8C%29 (Дата обращения 07.10.2014).

6. Максимов В.Ю. Незаконное обращение с вредоносными программами для ЭВМ: проблемы криминализации, дифференциации ответственности и индивидуализации наказания. Дис. ... канд. юрид. наук: 12.00.08. - Краснодар: РГБ, 1998. – 168 с.

7. Маслакова Е.А.. Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты. Дис. ... канд. юрид. наук: 12.00.08. - Орел: РГБ, 2008. – 198 с.

8. Ф-615 кн.1 - Сведения о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации. Сводный и сборник по России за январь-декабрь 2010 г. [Электронный ресурс] - Режим доступа: http:// giz. mvd. ru.

9. Ф-615 кн.1 - Сведения о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации. Сводный и сборник по России за январь-декабрь 2011 г. [Электронный ресурс] - Режим доступа: http:// giz. mvd. ru.

10. Ф-615 кн.1 - Сведения о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации. Сводный и сборник по России за январь-декабрь 2012 г. [Электронный ресурс] - Режим доступа: http:// giz. mvd. ru.

11. «О направлении статистических сведений»: письмо ФКУ «ГИАЦ МВД России» от 5.03.2014 г. исх.№ 34/4 – 158.

12. Чекунов И.Г. Некоторые особенности квалификации преступлений в сфере компьютерной информации / И.Г. Чекунов // Российский следователь. 2012. № 3. С.26-28.

13. Менжега М. М. Криминалистические проблемы расследования создания, использования и распространения вредоносных программ для ЭВМ. Дис. ... канд. юрид. наук: 12.00.09. - Саратов: РГБ, 2005. – 238 с.

14. Малыковцев М. М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ. Дис. ... канд. юрид. наук: 12.00.08. - М.: РГБ, 2007. – 186 с.

15. «Конвенция о преступности в сфере компьютерной информации» (ETS N 185) [рус., англ.] (Заключена в г. Будапеште 23.11.2001) // СПС КонсультантПлюс [Электронный ресурс] (Дата обращения 07.10.2014).

16. Волженкин Б.В. Преступления в сфере экономической деятельности по уголовному праву России. - СПб.: Изд-во Р.Асланова “Юридический центр Пресс”, 2007. - 763с. - (Теория и практика уголовного права и уголовного процесса).

17. Рарог А.И. Квалификация преступлений по субъективным признакам. – СПб.,2003. – 304 с.

18. Уголовно-правовое воздействие: монография / Г.А. Есаков, Т.Г. Понятовская, А.И. Рарог и др.; под ред. А.И. Рарога. М.: Проспект, 2014. - 288 с. (Автор главы - доктор юридических наук, профессор Г.А. Есаков).

PROBLEMS OF CRIMINAL-LEGAL QUALIFICATION OF CRIMES IN THE SPHERE OF COMPUTER INFORMATION

K.N. Evdokimov**,** candidate of legal Sciences, associate Professor, associate Professor of the Department of state and legal disciplines

Irkutsk law Institute (branch) of the Academy of the General Prosecutor of the Russian Federation, Irkutsk (Russia)

Annotation: The article is devoted to the issues of criminal-legal qualification of crimes in the sphere of computer information. The author carries out the analysis of the most pressing problems faced by law implementer qualification for the criminal acts of this kind, and makes proposals for improvement of the current criminal legislation.

Keywords: computer crime, crime in the sphere of computer information, illegal access to computer information, computer programs, malicious computer programs.

УДК 342

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ПО СУДЕБНИКУ 1550 ГОДА: СУЩНОСТЬ И ЗНАЧЕНИЕ

М.В. Зейц**,** магистрант института права

В.Г. Медведев**,** доктор юридических наук, доцент, заведующий кафедрой «История государства и права»

Тольяттинский государственный университет, Тольятти (Россия)

Аннотация. В статье рассматриваются вопросы деяний, нарушающих частный интерес по Судебнику 1550 г. Определяется их сущность и значение в формировании законодательной базы соответствующего периода. Указывается на их особенности и влияние на государственном уровне.

Ключевые слова: душегубство, система суда, Судебник, законодатель, деяния.

Обращаясь к истории возникновения Судебника, необходимо подчеркнуть, что его появление обусловлено государственной необходимостью того периода, так как в первой половине XVI века Московское государство столкнулось с настоящим кризисом государственности. Судебник 1550 был создан в первые годы самостоятельного правления Ивана IV, данный шаг явился правовой основой оздоровления государственной системы суда производства, повлиявшего на изменения взаимоотношений основных социальных групп. Судебником 1550 года были закреплены интересы широких слоёв общества.

Так Н.П. Загоскин, известный историк права, высказался об этой черте Судебника следующим образом «Во всех вообще статьях, во всех определениях нового Судебника, ясно просвечивает крайне недоверчивое, крайне подозрительное отношение законодателя к правительственным должностным лицам; это не покажется удивительным, коль скоро примем мы в соображение крайне неудовлетворительное состояние современного суда и администрации и тягостные для народа неурядицы эпохи правления бояр в малолетство