УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
Том 149, кн. 6 Гуманитарные науки *2007*

УДК 343

ОБЪЕКТИВНЫЕ И СУБЪЕКТИВНЫЕ ПРИЗНАКИ СОЗДАНИЯ И РАСПРОСТРАНЕНИЯ ВРЕДОНОСНЫХ ПРОГРАММ ДЛЯ ЭВМ

М.А. Зубова

Аннотация

В статье с учетом сложившейся правоприменительной практики рассматривается объект, объективная сторона, субъект и субъективная сторона преступления, предусмотренного статьей 273 Уголовного кодекса Российской Федерации. При анализе указанных признаков выявляется несовершенство статьи. Предлагается внести изменения в диспозицию, которые бы позволили сделать норму соответствующей современным условиям, повысить количественные показатели относительно выявления данного преступления.

Статья 273 УК РФ предусматривает ответственность за создание, использование и распространение вредоносных программ для ЭВМ, т. е. программ, заведомо приводящих к несанкционированному копированию, уничтожению, модификации, блокированию информации, нарушению работы ЭВМ, системы ЭВМ, их сети, а также внесение изменений в существующие программы, придающих им аналогичные опасные свойства. Статья 273 УК РФ стала преемницей ст. 269 проекта действующего Уголовного кодекса – «Создание, использование и распространение вирусных программ». Смена дефиниций произошла вследствие того, что под «компьютерным вирусом» в теории программирования понимается такая совокупность машинного кода, которая сама может создавать свои копии и внедрять их в файлы, системные области ЭВМ, вычислительные сети и т. д. При этом копии не обязательно полностью совпадают с оригиналом, могут становиться совершеннее его и сохраняют способность дальнейшего самораспространения [1, с. 12].

Данный вид преступлений получил довольно широкое распространение в России, особенно с ростом числа российских пользователей интернета, значительная часть которых уже испытала на себе действия подобных программ. По степени возможного причинения вреда компьютерные вирусы варьируются от «почти безобидных», изредка дающих знать о себе какими-либо сообщениями с непристойным содержанием, до опасных, способных привести к полной потере информации на носителе и даже к выводу из строя аппаратной части ЭВМ. Однако вредоносность программ определяется не характером их деструктивных возможностей, а тем, что все действия производятся несанкционированно, т. е. без уведомления пользователя, скрытно от него. В этом основное

отличие вредоносных программ от иных, которые также могут производить копирование, уничтожение, модификацию информации.

Непосредственным объектом данного преступления являются общественные отношения по обеспечению безопасности компьютерной информации, а также безопасности функционирования программ для ЭВМ.

Объективная сторона рассматриваемого преступления характеризуется действием – созданием вредоносной программы или внесением изменений в существующие программы, использованием или распространением таких программ или машинных носителей с такими программами. В законодательстве [2] под программой для ЭВМ понимается «объективная форма представления данных и команд, предназначенных для функционирования электронных вычислительных машин и других компьютерных устройств с целью получения определенного результата». По мнению М.Ю. Дворецкого, вредоносной программой является программа, заведомо разработанная или модифицированная для дальнейшего несанкционированного собственником или владельцем ЭВМ, системы ЭВМ или их сети уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ [3, с. 76]. А.Е. Шарков считает, что «вредоносная программа – это программа, приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, их системы или сети» [4, с. 129]. В.В. Воробьев полагает, что вредоносной программой является «программное средство, которое было создано для выполнения несанкционированных собственником и другими законными владельцами информации, ЭВМ, системы ЭВМ или их сети функций» [5, с. 58]. Вредоносная программа – это прежде всего программа для ЭВМ. Определение программы для ЭВМ дано в ст. 1261 ГК РФ, под которой понимается представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения. Вредоносная программа отличается от других программ для ЭВМ своими свойствами. Таким образом, вредоносной программой следует считать представленную в объективной форме совокупность данных и команд, предназначенных для ЭВМ и других компьютерных устройств в целях получения определенного результата, в виде уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети, а также других негативных последствий. Для четкого и единообразного понимания понятия «программа для ЭВМ», приведения законодательства в соответствие с частью четвертой ГК РФ его необходимо вынести в примечание к ст. 273.

В.В. Воробьев под созданием вредоносной программы понимает «продолжаемый процесс, который начинается с возникновения идеи, продолжается определением основных принципов работы программы, затем пишется исходный текст программы и заканчивается процесс создания программы ее компилированием» [5, с. 99]. М.Ю. Дворецкий указывает, что «создание вредоносных программ – это целенаправленная деятельность, которая включает в себя: 1) постановку задачи, определение среды существования и цели программы; 2) выбор

средств и языков реализации программы; 3) написание непосредственно текста программы; 4) отладку программы; 5) запуск и работу программы. Любое из перечисленных действий охватывается признаками создания вредоносной программы и может быть признано преступлением, предусмотренным ч. 1 ст. 273 УК, даже в том случае, когда вредоносная программа еще не создана, а находится, так сказать, еще в стадии оформления» [3, с. 79]. Данная позиция не верна, так как, не будучи должным образом «оформленной», вредоносная программа не будет представлять опасности. Вредоносная программа будет считаться созданной с того момента, когда последовательность команд станет пригодной для непосредственного выполнения без какого-либо предварительного преобразования. Существует точка зрения, согласно которой созданием программы может считаться также запись ее текста на бумаге. Однако сам по себе текст не несет никакой, даже потенциальной опасности, пока не будет кем-либо переведен в машинный код (в противном случае, вредными можно признать ряд учебников по программированию), кроме того, написание программ с заданными свойствами без их тестирования и отладки под силу лишь узкому кругу специалистов. Следует отметить тот факт, что вредоносные программы не всегда создаются с целью причинить вред в будущем. Так, официальным заданием для студентов Ульяновского государственного технического университета является создание компьютерного вируса, а также нейтрализующей его программы. Поэтому целесообразно указать в законе на цели создания программы, так как сам факт ее создания никаких негативных последствий не влечет. Как справедливо указывает С.Ю. Ушаков, «законодатель использует в диспозиции ст. 273 УК в описании предмета преступления множественное число, из чего может создаться впечатление об одновременной необходимости для уголовной ответственности за это преступление создания, использования и распространения не одной, а нескольких вредоносных программ или машинных носителей с такими программами. 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 УК РФ возможно уже в случаях создания, использования и распространения одной вредоносной программы для ЭВМ или одного машинного носителя с такой программой» [6, с. 117].

Таким образом, часть первую статьи 273 УК РФ следует изложить в следующей редакции:

«Создание программы для ЭВМ с целью несанкционированного уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети, а также внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети, а равно их использование либо распространение машинных носителей с такой программой».

Внесение изменений в существующие программы – модификация информации, понятие которой рассматривалось в предыдущем параграфе. Однако

изменения лицом вносятся умышленно, с целью наступления последствий в виде уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети.

Под использованием вредоносной программы М.Ю. Дворецкий понимает «такие действия, которые обеспечивают непосредственный их выпуск, воспроизведение, распространение и иные операции по введению их в хозяйственный оборот» [3, с. 79]. В.В. Воробьев под использованием вредоносных программ понимает «применение этих программ по прямому назначению» [5, с. 94]. Под использованием вредоносной программы следует понимать запуск такой программы в ЭВМ, системе ЭВМ или их сети.

Под распространением вредоносной программы понимается ее передача как с помощью специальных носителей, сети, так и иным другим способом другому лицу. Например: Краснооктябрьский суд г. Волгограда осудил Гугняева за совершение преступления, предусмотренного ч. 1 ст. 273 УК РФ. Гугняев на одном из рынков г. Волгограда реализовал компьютерный диск «Супер-Хакер», заведомо зная, что данные диск содержит вредоносные программы для ЭВМ. Наряду с информацией технического характера, диск содержал исполнимые файлы вредоносных компьютерных программ, приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ. Было обнаружено 9 опасных вирусов, приводящих при заражении к уничтожению информации на жестком диске компьютера, 45 неопасных вирусов, занимающих ресурсы компьютера и могущих вызвать ошибки и сбои программного обеспечения[1].

Распространение вредоносных программ может осуществляться наряду с другим преступлением или для подготовки к нему. Например: Ленинским районным судом г. Ульяновска К. был осужден по ст. 272 ч. 2, 273 ч. 1, 183 ч. 1, 2 УК РФ. Действуя из корыстных побуждений, с целью бесплатного доступа к сети интернет и причинения крупного ущерба ООО «Берег», незаконного доступа к охраняемой законом компьютерной информации ООО «Берег», завладения логином и паролем, использования и распространения вредоносных программ для ЭВМ, а также собирания, разглашения сведений, составляющих коммерческую тайну предприятия, скрытно установил в базу данных компьютера предприятия программу «Троянский конь», с помощью которой завладел логином и паролем законного пользователя, т. е. ООО «Берег». Затем К., используя данный логин и пароль неоднократно соединялся с сервером провайдера ОАО «Ульяновск-электросвязь» и неправомерно получал доступ к сети интернет. Действиями К. ООО «Берег» был причинен материальный ущерб. Имея необходимый логин и пароль, К. имел доступ к электронному почтовому ящику предприятия, предназначенного для передачи электронной почты конфиденциального и коммерческого характера, который находился в компьютерной системе провайдера. К. регулярно производил копирование электронных почтовых сообщений, содержащих сведения о торговых партнерах, имуществе, ценной политике на рынке и другую информацию, составляющую коммерческую тайну, чем причинил ООО «Берег» крупный ущерб. Данные о незаконно добытом

[1] По материалам http//:www.crime-research.ru.

логине и пароле были переданы знакомому К. – А., которому не было известно об их незаконности. А. с помощью своего домашнего ПК также выходил в интернет, в связи с чем ООО «Берег» был причинен материальный ущерб на сумму свыше 7 тыс. руб.

Ч. был осужден за совершение преступлений, предусмотренных ст. 242 и 273 ч. 1 УК РФ. То есть Ч. незаконно распространил и рекламировал порнографические материалы, а также распространил вредоносные программы для ЭВМ, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети. Используя свой ПК, модем и домашний телефон, Ч. установил и настроил к работе телекоммуникационный узел – любительскую станцию, предоставив услуги к ее подключению неограниченному кругу пользователей. Ч. умышленно разместил в информационном пространстве картинки порнографического содержания, а также 118 вредоносных программ для ЭВМ, которые были умышленно распространены им пользователям станции [7].

С субъективной стороны преступление, предусмотренное ч. 1 ст. 273 характеризуется умышленной виной в виде прямого умысла. О характере субъективной стороны свидетельствует указание в законе на заведомость для виновного наступления общественно опасных последствий в результате создания, использования или распространения вредоносных программ [8, с. 463].

Субъект данного преступления – вменяемое лицо, достигшее 16 лет.

Часть 2 ст. 273 в качестве квалифицирующего признака указывает причинение по неосторожности тяжких последствий. При этом «тяжкие последствия» – оценочная категория, которая подлежит квалификации судом. Согласно п. 8 постановления Пленума Верховного Суда Российской Федерации от 29 апреля 1996 г. № 1 суд, признавая подсудимого виновным в совершении преступления по признакам, относящимся к оценочным категориям (тяжкие или особо тяжкие последствия, крупный или значительный ущерб, существенный вред, ответственное должностное положение подсудимого и др.), не должен ограничиваться ссылкой на соответствующий, а обязан привести в описательной части приговора обстоятельства, послужившие основанием для вывода о наличии в содеянном указанного признака. Как справедливо указывает С.Д. Бражник: «Изучение юридической литературы показало, что в оценке «тяжких последствий» применительно к исследуемым составам сложились два подхода. Приверженцы первого подхода понимают под ними потерю исключительно важной информации, незаменимую информацию, наличие которой обеспечивает функционирование ЭВМ, системы ЭВМ или их сети, а также информацию, необходимую для функционирования физического или юридического лица; важную информацию – информацию, которая может быть заменена, но это связано с большими затратами и трудностями; информацию, которая приносит очевидную пользу и которую довольно трудно восстановить, хотя ЭВМ, система ЭВМ или их сеть, а также юридическое или физическое лицо могут нормально функционировать и без нее. Большинство же ученых тяжкие последствия трактуют так: это «гибель людей, причинение вреда здоровью, дезорганизация производства на предприятии или в отрасли промышленности, осложнение дипломати-

ческих отношений с другим государством, возникновение вооруженного конфликта» [9, с. 140]. В примечании к ст. 273 или в тексте самой статьи необходимо указать примерный перечень таких последствий, как это сделано в УК Республики Беларусь. Состав считается оконченным с момента наступления указанных последствий.

С субъективной стороны преступление характеризуется двойной формой вины: прямым умыслом по отношению к действиям и неосторожностью (как в виде легкомыслия, так и небрежности) – к наступлению тяжких последствий. Вопрос о так называемой двойной – «сложной», или «смешанной», – форме вины на протяжении многих лет был дискуссионным в науке уголовного права. Подавляющее большинство ученых-криминалистов и практических работников пришли к выводу, что такие наименования не совсем удачны, ибо вина всегда едина и всегда выступает в виде умысла или неосторожности. Но встречаются ситуации, предусмотренные отдельными статьями УК, когда наступление тяжких последствий отягчает содеянное и представляет собой квалифицированный вид данного преступления. При этом, если основной состав преступления с субъективной стороны характеризуется виной умышленной, то отношение виновного к тяжким последствиям, предусмотренным квалифицированным составом данного преступления, характеризуется неосторожностью [10, с. 57].

По данным статистического отчета МВД РФ, количество зарегистрированных преступлений, предусмотренных ст. 273 УК РФ, в 2003 г. составило 700, в 2004 г. – 1020, в 2005 г. – 1890. Однако количество выявленных лиц в 2003 г. составило 88 человек, в 2004 г. – 100, в 2005 г. – 119. Налицо большой разрыв между количеством зарегистрированных преступлений и выявленных лиц. Одной из причин, на наш взгляд, является несовершенство действующей нормы. Необходимо ее модернизировать, например, так, как указано выше.

Summary

M.A. Zubova. Objective and subjective attributes of creating and spreading harmful computer programs.

The article views object, objective side, subject, and subjective side of crime set in article 273 of the Criminal Code of the Russian Federation, with regard to the existing law-enforcement practice. The analysis of features specified displays the article imperfection. Changes to the disposition are offered, which allow conforming the norm to modern conditions, as well as increasing quantification of crime case revealing.

Литература

1. *Ляпунов В., Максимов В.* Ответственность за компьютерные преступления // Законность. – 1997. – № 1. – С. 8–15.
2. Ведомости Съезда народных депутатов РФ и Верховного Совета РФ. – 1992. – № 42. – Ст. 2325.
3. *Дворецкий М.Ю.* Преступления в сфере компьютерной информации (уголовно-правовое исследование): Дис. … канд. юрид. наук. – Волгоград, 2001. – 109 с.
4. *Шарков А.Е.* Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации: Дис. … канд. юрид. наук. – Ставрополь, 2004. – 174 с.

5. *Воробьев В.В.* Преступления в сфере компьютерной информации (юридическая характеристика составов и квалификация): Дис. … канд. юрид. наук. – Н. Новгород, 2000. – 201 с.
6. *Ушаков С.Ю.* Преступления в сфере компьютерной информации (теория, законодательство, практика): Дис. … канд. юрид. наук. – Ростов н/Д, 2000. – 176 с.
7. Архив Ленинского районного суда г. Ульяновска. – 1999.
8. Российское уголовное право: в 2 т. Т. 2. Особенная часть / Под ред. Л.В. Иногамовой-Хегай, В.С. Комиссарова, А.И. Рарога. – М.: ТК Велби, Проспект, 2006. – 656 с.
9. *Бражник С.Д.* Преступления в сфере компьютерной информации: проблемы законодательной техники: Дис. … канд. юрид. наук. – Ижевск, 2002. – 189 с.
10. Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. А.И. Рарог. – М.: Проспект, 2004. – 639 с.

Поступила в редакцию
29.08.07

Зубова Марина Александровна – аспирант кафедры уголовного права Казанского государственного университета.