УДК 343.533

ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Лысак Елена Андреевна
к.ю.н., старший преподаватель кафедры уголовного права Кубанского Государственного Аграрного Университета

Кубанский Государственный Аграрный Университет, Краснодар, Россия

Статья посвящена некоторым проблемам, возникающим при квалификации преступлений в сфере компьютерной информации. Приведены различные точки зрения, и на их основании предложены способы совершенствования действующего законодательства. Рассмотрены некоторые положительные изменения российского законодательства

Ключевые слова: ПРЕСТУПНОСТЬ, ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ, УГОЛОВНОЕ ЗАКОНОДАТЕЛЬСТВО, ЗАРУБЕЖНОЕ ПРАВО

UDC 343.533

PROBLEMS OF QUALIFICATION OF COMPUTER CRIMES

Lysak Elena Andreevna
Cand.Leg.Sci., senior lecturer of the Criminal Law Department of Kuban State Agrarian University

Kuban State Agrarian University, Krasnodar, Russia

The article is dedicated to some troubles witch arising in the qualification of crimes in the sphere of computer information. It shows the different points of view, and, on this base, proposes the ways of improving current legislation. Some positive changes of the Russian legislation are considered

Keywords: CRIMINALITY, COMPUTER CRIMES, CRIMINAL LEGISLATION, FOREIGN LAW

В информационном обществе важное место занимают компьютерные системы, так как они способны обрабатывать информацию из различных источников. К сожалению, компьютеризация имеет не только положительные, но также и отрицательные стороны. В первую очередь к негативным моментам относится появление новых видов преступности, а именно – преступлений в сфере компьютерной информации.

Законодательная практика ряда наиболее развитых государств идет по пути ужесточения законодательства, посвященного компьютерным преступлениям[3]. Недавние изменения УК РФ[1] также свидетельствуют об усилении уголовной ответственности за такие преступления.

Поместив главу 28 в раздел IX УК, законодатель определил родовой объект рассматриваемых преступлений как отношения общественной безопасности. По мнению ряда ученых, видовым объектом этих

преступлений будет являться информационная безопасность как вид общественной безопасности, т.е. отношения по безопасному производству, хранению, использованию или распространению информации и информационных ресурсов[13].

Основным объектом этих преступлений являются общественные отношения, обеспечивающие безопасность и конфиденциальность компьютерной информации. Факультативным объектом являются личные права граждан, права законных обладателей программ для ЭВМ и баз данных, неприкосновенность частной сферы, отношения собственности, общественная и государственная безопасность.

Предметом этой группы преступлений является хранящаяся и обрабатываемая в компьютерных системах информация. Она может оказаться объектом преступления; являться средством совершения преступления по отношению к информации на других компьютерах либо свидетельствовать об иной преступной деятельности[4].

Легальное определение информации дано в ФЗ «Об информации, информационных технологиях и о защите информации» [2], в соответствии с которым под информацией понимаются сведения (сообщения, данные) независимо от формы их представления.

В свою очередь, понятие «компьютерная информация» раскрывается непосредственно в тексте уголовного закона. Согласно примечанию 1 к ст. 272 УК, под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Это понятие было ведено в декабре 2011 года. Положительным является приведение понятия компьютерной информации в соответствие с определением информации, указанном в ФЗ «Об информации, информационных технологиях и о защите информации». Такое изменение уголовного закона можно назвать последовательным и системным. Оно разрешает

существовавшие ранее трудности в понимании термина «компьютерная информации» и устраняет внутреннюю несогласованность российского законодательства.

В ст. 272 УК «Неправомерный доступ к компьютерной информации» установлено наказание за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации. Отдельные авторы не согласны с названием ст. 272 УК, так как считают, что исходя из диспозиции, правильнее было бы говорить о неправомерном воздействии на информационную систему[8]. С этим сложно согласиться, так как обозначение статьи в целом соответствует ее внутреннему наполнению, и при квалификации преступления важен не заголовок статьи, а содержание диспозиции нормы.

Состав преступления в ст. 272 УК является материальным. Уголовный закон не дает определения неправомерного доступа к охраняемой законом компьютерной информации, а указывает лишь его последствия. Отсутствие законодательного определения неправомерного доступа вызывает трудности при квалификации деяния по ст. 272 УК[12].

Неправомерный доступ достигается путем проникновения в компьютерную систему или носители информации при помощи специальных технических или программных средств, незаконного использования паролей и иных данных.

Неправомерным также считают доступ к информационным ресурсам сети Интернет без согласия собственника или иного законного владельца охраняемой законом информации, если это привело к уничтожению, блокированию, модификации или копированию информации, при обязательном условии отсутствия у лица права доступа к ней[7].

Сам факт вызова или просмотра компьютерной информации, хранящейся на машинном носителе, состава такого преступления не

образует[10]. Дискуссионным является такой обязательный признак объективной стороны неправомерного доступа к компьютерной информации как общественно опасные последствия. Законодатель не раскрывает понятия конкретных видов последствий, указанных в диспозиции статьи. Данные опроса сотрудников правоохранительных органов показывают, что это затрудняет процесс квалификации[15].

В теории уголовного права под уничтожением информации понимается утрата информации при невозможности ее восстановления. Блокирование информации – это невозможность ее использования при сохранности такой информации. Модификация информации означает изменение ее содержания по сравнению с той информацией, которая первоначально была в распоряжении собственника или законного пользователя. Под копированием информации следует понимать ее переписывание, а также иное тиражирование при сохранении оригинала[9].

Одним из особо квалифицирующих признаков этого состава преступления является наступление тяжких последствий или создание угрозы их наступления в результате неправомерного доступа к компьютерной информации. Эта часть статьи (ч. 4) также является относительно новой. Признак наступления тяжких последствий необходим в этом составе преступления, так как с развитием компьютерных технологий появляется и больше возможностей совершения противоправных деяний в этой сфере. Многие процессы в функционировании современного общества автоматизированы, в связи с чем, при неправомерном доступе к компьютерной информации велика вероятность причинения вреда большому количеству людей.

В ст. 273 УК РФ установлена ответственность за создание, использование и распространение вредоносных компьютерных программ.

Вредоносной программой является программное средство, которое было создано для выполнения несанкционированных собственником и другими законными пользователями информации, компьютера или компьютерной системы или сети их сети функций. Вредоносность программы определяется не только способностью уничтожать, блокировать, модифицировать или копировать информацию. Особенностью вредоносных программ является то, что они выполняют эти функции без уведомления или получения согласия законного владельца информации[6].

Объективная сторона преступления выражается в альтернативных действиях: создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты.

Состав преступления сконструирован по типу формального. Для признания преступления оконченным не требуется реального наступления вредных последствий. Достаточно установить факт совершения общественно опасного деяния, если оно создавало реальную угрозу наступления перечисленных выше вредных последствий[14]. Именно высокой степенью общественной опасности объясняется то, что уголовный закон достаточно строго преследует за сам факт создания таких компьютерных программ.

В ст. 274 УК РФ предусмотрена ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Объективная сторона преступления описывается с использованием приема бланкетности, в соответствии с которым указание в диспозиции на

деяние носит обобщенный характер – «нарушение правил» [11]. Незаконным признается нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям. Обязательным признаком являются последствия в виде уничтожения, блокирования, модификации либо копирования компьютерной информации, а также причинение крупного ущерба.

Диспозиция отсылает к инструкциям и положениям, устанавливающим правила эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей на предприятии, в учреждении и организации. Данные правила должны быть установлены уполномоченным лицом и в надлежащем порядке[5].

В науке уголовного права отмечается, что наиболее спорны в системе рассматриваемых преступлений нормы, содержащиеся в ст. 274 УК. Это связано с тем, что сегодня нет единых правил, определяющих порядок защиты информации, которые служили бы правовой основой для правильной квалификации деяния. Ряд исследователей предлагает принять подзаконный нормативно-правовой акт, который бы содержал правила, определяющие порядок защиты информации[7].

Необходимо отметить положительные сдвиги российского уголовного закона. Недавние изменения статей о преступлениях в сфере компьютерной информации явились серьезным шагом на пути совершенствования указанных норм. В частности, были исключены признаки, вызывающие множество трудностей при применении норм: «нарушение работы ЭВМ, системы ЭВМ или их сети», «совершение деяния лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети». В

диспозиции статей были внесены несколько важных и необходимых на сегодняшний день признаков: «наступление тяжких последствий или угроза их наступления», «совершение деяния из корыстной заинтересованности», «причинение крупного ущерба». В примечании к ст. 272 УК было закреплено толкование признака «крупный ущерб». Ранее используемое в ст. 274 УК понятие «существенный вред» не раскрывалось, что затрудняло применение нормы. Также, о чем уже говорилось ранее, было введено понятие «компьютерная информация».

Преступления, совершаемые в сфере компьютерной информации, представляют собой распространенное противоправное явление, и их число с каждым годом будет только увеличиваться. Это связано, прежде всего, с развитием компьютерной техники и программного обеспечения. Такие тенденции неизбежны. Со временем информационные технологии проникнут практически во все сферы преступной деятельности. В связи с этим, законодателю следовало бы ввести квалифицирующие признаки в те составы преступлений, которые часто совершаются с использованием компьютерных технологий. Это касается, в первую очередь, преступлений против собственности, против общественной безопасности, в сфере экономической деятельности, против конституционных прав и свобод человека и гражданина.

Первый шаг в этом направлении уже сделан. В частности, были внесены дополнения в состав мошенничества. Один из новых составов мошенничества был сформулирован законодателем в статье 159.6 УК РФ как «Мошенничество в сфере компьютерной информации». В данной норме закрепляется ответственность за мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или

передачи компьютерной информации или информационно-коммуникационных сетей.

Применение такого нововведения на практике поможет избежать многих сложностей, возникающих в процессе квалификации преступлений в сфере компьютерной информации. До принятия соответствующих поправок мошенничество путем неправомерного доступа к компьютерной информации требовало квалификации по совокупности преступлений, предусмотренных статьями 159 и 272 УК РФ. Таким образом, в действиях виновного налицо были признаки идеальной совокупности преступлений. Получалось, что одним действием лицо совершало два преступления. В настоящее время, с учетом внесенных изменений, достаточно будет применения статьи 159.6 УК, что свидетельствует об упрощении процесса уголовного судопроизводства, и о своеобразной экономии средств уголовной репрессии.

В дальнейшем, было бы правильным ввести квалифицирующий признак «совершение преступления с использованием компьютерных технологий» и в ряд других составов преступлений, в частности, в составы нарушения авторских и смежных прав, кражи, причинения имущественного ущерба путем обмана или злоупотребления доверием и ряд других.

В заключении нужно отметить, что внедрение информационных систем практически во все сферы жизни общества создало предпосылки использования этих процессов для совершения преступлений. Соответственно, в результате быстрого развития новых технологий не менее быстрыми темпами развиваются и формы преступной деятельности. Исходя из вышеизложенного, можно с уверенностью утверждать о необходимости дальнейшего совершенствования норм российского законодательства об ответственности за преступления в сфере компьютерной информации.

Литература

1.Уголовный кодекс РФ от 13.06.1996 N 63-ФЗ (ред. от 05.04.2013) // Собрание законодательства РФ, 17.06.1996, N 25, ст. 2954.

2.Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ от 31 июля 2006 г. N 31 (1 ч.). Ст. 3448.

3.Бытко С. Ю. Некоторые проблемы уголовной ответственности за преступления, совершаемые с использованием компьютерных технологий. Дис. … канд. юрид. наук. Саратов, 2002. 207 с.

4.Гаврилов М., Иванов А. Извлечение и исследование компьютерной информации // Криминалистика. 2004. № 4. С. 74

5.Комментарий к Уголовному кодексу Российской Федерации / Авт. кол.: А. Е. Беляев, Г. Н. Борзенков, В. П. Верин и др.; Отв. ред. В. И. Радченко; Науч. ред. А. С. Михлин; Верховный Суд Российской Федерации. – СПб.: Питер, 2008. – 784 с.

6.Комментарий к Уголовному кодексу Российской Федерации (отв. ред. А. А. Чекалин; под ред. В. Т. Томина, В. В. Сверчкова). - 3-е изд., перераб. и доп. - Юрайт-Издат, 2006 г. С. 220.

7.Копырюлин А. Н. Квалификация преступлений в сфере компьютерной информации // Законность, 2007, N 6. С. 40.

8.Осипенко А. Уголовная ответственность за неправомерный доступ к конфиденциальной компьютерной информации // Уголовное право, 2007, N 3. С. 43-37

9.Постатейный Комментарий к Уголовному кодексу РФ 1996 г. (под ред. Наумова А. В.) - "Гардарика", "Правовая культура" 1996 г.

10.Расследование неправомерного доступа к компьютерной информации / Под ред. Н. Г. Шурухнова. М.: Щит-М, 1999. С. 70.

11.Российское уголовное право: в 2 т. Т. 2. Особенная часть: учебник / Г. Н. Борзенков [и др.]; под ред. Л. В. Иногамовой-Хегай, В. С. Комисарова, А. И. Рарога. – 3-е изд. перераб. и доп. – Москва: Проспект, 2011. – 688 с. С. 492.

12.Сизов А. В. Неправомерный доступ к компьютерной информации: практика правоприменения // Информационное право. 2009. N 1. С. 32-35.

13.Уголовное право Российской Федерации. Особенная часть: Учебник / Под ред. проф. Б. В. Здравомыслова. - Изд. 2-е, перераб. и доп. М., 2001.

14.Ястребов Д. А. Вопросы отграничения неправомерного доступа к компьютерной информации от смежных составов преступлений // Российский следователь. 2008. N 17. С. 25-26.

15.Ястребов Д. А. Общественно опасные последствия неправомерного доступа к компьютерной информации: нарушения работы ЭВМ, системы ЭВМ или их сети // Правовые вопросы связи, 2009, N 1 // СПС «КонсультантПлюс»

References

1. Ugolovnyj kodeks RF ot 13.06.1996 N 63-FZ (red. ot 05.04.2013) // Sobranie zakonodatel'stva RF, 17.06.1996, N 25, st. 2954.

2. Federal'nyj zakon ot 27.07.2006 N 149-FZ «Ob informacii, informacionnyh tehnologijah i o zashhite informacii» // Sobranie zakonodatel'stva RF ot 31 ijulja 2006 g. N 31 (1 ch.). St. 3448.

3. Bytko S. Ju. Nekotorye problemy ugolovnoj otvetstvennosti za prestuplenija, sovershaemye s ispol'zovaniem komp'juternyh tehnologij. Dis. … kand. jurid. nauk. Saratov, 2002. 207 s.

4. Gavrilov M., Ivanov A. Izvlechenie i issledovanie komp'juternoj informacii // Kriminalistika. 2004. № 4. S. 74.

5. Kommentarij k Ugolovnomu kodeksu Rossijskoj Federacii / Avt. kol.: A. E. Beljaev, G. N. Borzenkov, V. P. Verin i dr.; Otv. red. V. I. Radchenko; Nauch. red. A. S. Mihlin; Verhovnyj Sud Rossijskoj Federacii. – SPb.: Piter, 2008. – 784 s.

6. Kommentarij k Ugolovnomu kodeksu Rossijskoj Federacii (otv. red. A. A. Chekalin; pod red. V. T. Tomina, V. V. Sverchkova). - 3-e izd., pererab. i dop. - Jurajt-Izdat, 2006 g. S. 220.

7. Kopyrjulin A. N. Kvalifikacija prestuplenij v sfere komp'juternoj informacii // Zakonnost', 2007, N 6. S. 40.

8. Osipenko A. Ugolovnaja otvetstvennost' za nepravomernyj dostup k konfidencial'noj komp'juternoj informacii // Ugolovnoe pravo, 2007, N 3. S. 43-37.

9. Postatejnyj Kommentarij k Ugolovnomu kodeksu RF 1996 g. (pod red. Naumova A. V.) - "Gardarika", "Pravovaja kul'tura" 1996 g.

10. Rassledovanie nepravomernogo dostupa k komp'juternoj informacii / Pod red. N. G. Shuruhnova. M.: Shhit-M, 1999. S. 70.

11. Rossijskoe ugolovnoe pravo: v 2 t. T. 2. Osobennaja chast': uchebnik / G. N. Borzenkov [i dr.]; pod red. L. V. Inogamovoj-Hegaj, V. S. Komisarova, A. I. Raroga. – 3-e izd. pererab. i dop. – Moskva: Prospekt, 2011. – 688 s. S. 492.

12. Sizov A. V. Nepravomernyj dostup k komp'juternoj informacii: praktika pravoprimenenija // Informacionnoe pravo. 2009. N 1. S. 32-35.

13. Ugolovnoe pravo Rossijskoj Federacii. Osobennaja chast': Uchebnik / Pod red. prof. B. V. Zdravomyslova. - Izd. 2-e, pererab. i dop. M., 2001.

14. Jastrebov D. A. Voprosy otgranichenija nepravomernogo dostupa k komp'juternoj informacii ot smezhnyh sostavov prestuplenij // Rossijskij sledovatel'. 2008. N 17. S. 25-26.

15. Jastrebov D. A. Obshhestvenno opasnye posledstvija nepravomernogo dostupa k komp'juternoj informacii: narushenija raboty JeVM, sistemy JeVM ili ih seti // Pravovye voprosy svjazi, 2009, N 1 // SPS Konsul'tantPljus