Компьютерная информация как предмет преступления, предусмотренного статьей 273 Уголовного кодекса Российской Федерации

А.А. Энгельгардт

доцент кафедры уголовного права факультета права Национального исследовательского университета «Высшая школа экономики», кандидат юридических наук. Адрес: 101000, Российская Федерация, Москва, ул. Мясницкая, д. 20. E-mail: aengelgardt@hse.ru

Аннотация

Уголовно-правовая оценка создания, использования и распространения вредоносных компьютерных программ (информации) (ст. 273 Уголовного кодекса Российской Федерации (далее — УК РФ)) — необходимый элемент защиты одного из ведущих принципов регулирования сферы информации. В специальном законодательстве он сформулирован как свобода поиска, получения, передачи, производства и распространения информации любым законным способом. Факты свидетельствуют, что осмысленное, взвешенное и основанное на согласии понимание смысла запрета ст. 273 УК РФ и других деяний (ст. 141, 171^2, 185^3, 242, 272 УК РФ и др.), если они совершены посредством вмешательства в функционирование ЭВМ и/или информационно-телекоммуникационных сетей, зависит от понимания компьютерной информации как предмета соответствующего преступления. Понимания, которое выходит за рамки компетенции специалиста в области уголовного права. В связи с этим анализ понятия компьютерной информации — не просто дань лингвистическому педантизму, проявленному при исследовании компьютерных преступлений. Эта проблематика должна всесторонне исследоваться в юридической литературе, причем с различных позиций. В статье показывается, что понятийная характеристика компьютерной информации в УК РФ постоянно расширяется. Во-первых, она определена общим образом как сведения (сообщения, данные), представленные в форме электрических сигналов, доступных электронным устройствам, в том числе для передачи по информационным каналам связи. Согласно полученному эмпирическому материалу, это определение компьютерной информации не является прямым аргументом выводов постановлений и приговоров судов. Его роль обнаружилась в ином: оно позволяет теперь не связывать компьютерную информацию с определенными средствами ее хранения, обработки и передачи, обнаруживать ее во все большем числе технических устройств (банкоматах, ресиверах и др.). Исследование показывает, что в определение компьютерной информации отдельные статьи УК РФ вводят положения об особенных характеристиках (позитивные признаки), и (или) о том, почему та или иная информация не может быть оценена как предмет анализируемого состава преступления (негативные признаки). Поэтому, во-вторых, компьютерная информация как предмет определенного преступления обладает набором индивидуализирующих ее признаков. В ст. 273 УК РФ она представлена: а) в виде компьютерной программы или иной информации; б) которые заведомо предназначены для уничтожения, блокирования, модификации, копирования компьютерной информации либо нейтрализации средств ее защиты; в) когда на это отсутствует необходимая санкция. Отдельные из указанных признаков еще недостаточно исследованы. В частности, признак предназначенности компьютерной информации для нейтрализации средств ее защиты. В условиях повсеместного использования соответствующего технологического инструмента введение такого признака расширило объемы действия ст. 273 УК РФ и привело к примитивизации ее применения.

Ключевые слова

преступление, уголовная ответственность, предмет преступления, компьютерная информация, вредоносная компьютерная программа, нейтрализация средств защиты компьютерной информации

Библиографическое описание: Энгельгардт А.А. Компьютерная информация как предмет преступления, предусмотренного статьей 273 Уголовного кодекса Российской Федерации // Право. Журнал Высшей школы экономики. 2014. № 4. С. 136–145.

Современное общество основано на принципе свободы поиска, получения, передачи, производства и распространения информации любым законным способом[1]. Реализация здесь некоторых опасных незаконных приемов влечет уголовную ответственность[2]. Так, признается необходимым применение уголовного наказания за создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ)[3].

Крайне важно, чтобы каждое такое решение было осмысленным, взвешенным и основанным на согласии в понимании смысла действующего запрета. Деяния, подпадающие под признаки состава ст. 273 Уголовного кодекса Российской Федерации (далее — УК РФ), имеют отношение к области так называемых высоких технологий, но совершаются вместе с тем как в профессиональной, так и в обыденной поведенческих сферах, т.е. широко распространены. Отсюда и криминологические основания интереса к вопросам их уголовно-правовой оценки. По данным антивирусных компаний, которые могут быть, по понятным причинам преувеличены (а потому не переводимы прямо в разряд криминальной статистики), количество компьютерных атак (запусков программ для получения неавторизованного доступа к компьютерной сети и ее элементам) с российских интернет-ресурсов достигает десятков миллионов[4]. Евгений Касперский, директор «Лаборатории Касперского», утверждает: «Специалистам лаборатории известны более 35 тысяч программ, направленных на взлом компьютерных сетей, ежегодно злоумышленниками создаются около 200 тысяч новых компьютерных вирусов»[5]. Официальная статистика МВД дает следующую общую картину. В 2004 г. число зарегистрированных преступлений в сфере компьютерной информации достигло 13 723, затем без видимых причин снизилось в несколько раз — до 2563 в 2013 г.[6]

[1] См.: Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» // СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

[2] См.: Конвенция о преступности в сфере компьютерной информации (Будапешт, 23 ноября 2001 г.) // СПС «Гарант»; *Додонов В.Н., Капинус О.С., Щерба С.П.* Сравнительное уголовное право. Особенная часть: монография / под общ. ред. С.П. Щербы. М.: Юрлитинформ, 2010. С. 390.

[3] В литературе можно встретить утверждение, что упоминание о вредоносных программах изъято из ст. 273 УК РФ. См.: *Суслопаров А.В.* Эволюция института ответственности за компьютерные преступления // Эволюция государственных и правовых институтов в условиях развития информационного общества / отв. ред. И.Л. Бачило. М.: ИГП РАН; Юркомпани, 2012 // СПС «Гарант». Его действительно больше нет в диспозиции, но оно сохранено в названии статьи. В силу этого оно используется в работе как элемент юридической терминологии действующего закона.

[4] URL: http://www.securelist.com/ru/analysis/ (дата обращения: 14 ноября 2014 г.).

[5] URL: http://www.securitylab.ru/news/436955.php (дата обращения: 14 ноября 2014 г.).

[6] Официальный сайт Министерства внутренних дел Российской Федерации // URL: http://www.mvd.ru/presscenter/statistics/reports (дата обращения: 14 ноября 2014 г.).

Статья не является «драматически» недействующей, но качество ее применения вызывает скепсис. Оказалось, что оно в значительной степени зависит от активности правоохранительных органов. По крайней мере в изученном массиве более чем 90% дел такое преступление было выявлено в результате проведения оперативно-розыскных мероприятий[7]. Алгоритм действий сотрудников: звонок по указанному в размещенном в Интернете объявлении о ремонте компьютеров и установке программ, достижение договоренности, установка контрафактного экземпляра с помощью программ, обеспечивающих нейтрализацию средств защиты компьютерной информации, задержание виновного. Просто и результативно. Но применение запрета становится выборочным, хотя законодатель не приветствует такой возможности усмотрения правоприменителя.

С другой стороны, некоторые публикации в юридической литературе утверждают, что применение ст. 273 УК РФ связано с немалыми трудностями и требует принятия сложных решений[8]. Попытаемся выяснить это в контексте характеристики предмета исследуемого преступления.

По принятому мнению, ст. 273 УК РФ содержит формальный состав единичного сложного преступления, складывающего из так называемых альтернативных действий: создание, распространение или использование компьютерной информации, в том числе компьютерных программ, заведомо предназначенных для несанкционированного уничтожения, блокирование, модификация, копирование компьютерной информации или нейтрализация средств защиты компьютерной информации. Как видно, важнейшая роль в структуре объективных признаков состава принадлежит компьютерной информации. При этом ее признаки как предмета преступления даже более четко, чем его объект, выделяют преступление в целом, сужая пределы преступного деяния до охраняемой нормами гл. 28 УК РФ сферы компьютерной информации.

Определение компьютерной информации как предмета преступления непросто даже при том условии, что в примечании 1 к ст. 272 УК РФ закреплено ее нормативное понятие[9]. Ведь это сделано нестандартно. Введя тот или иной термин и закладывая в уголовный кодекс представление о нем, как общем для ряда составов, законодатель выбирает два пути. Один состоит в том, чтобы раскрыть понятие в определении, как правило, самым общим образом. Второй — в том, чтобы дать ряд хотя бы косвенных указаний, раскрывающих его содержание. Сначала УК РФ в ст. 272 указывал как признаки компьютерной информации определенные средства ее хранения, обработки и передачи — машинный носитель, электронно-вычислительную машину (ЭВМ), систему ЭВМ или их сеть. В новой редакции норм гл. 28 УК РФ, по сути, несколько определений компьютерной информации. Первое — общее понятие, вынесено из диспозиции в примечание к ст. 272 УК РФ.

---

[7] Материалом для изучения послужила судебная практика 2013–2014 гг., опубликованная на сайте URL:http://rospravosudie.com. Всего было изучено 50 судебных актов, вынесенных по ст. 273 УК РФ.

[8] См., напр.: *Дворецкий М., Копырюлин А.* Проблемы квалификации преступлений, сопряженных с созданием, использованием и распространением вредоносных программ // Уголовное право. 2007. № 4. С. 29–33.

[9] Цель статьи ограничена анализом компьютерной информации как предмета преступления. За рамками анализа остается проблема использования компьютерной информации в качества средства совершения преступления (мошенничества и др.). Ответственность за преступления, где компьютерная информация служит уже средством совершения преступления, должна наступать по статьям иных глав УК РФ в соответствии с непосредственным объектом посягательства.

Согласно примечанию, компьютерная информация — это сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Такое понимание предмета оказывается только исходным. Далее, особенно при правоприменении, оно дополняется позитивными признаками (суждениями, каковы характеристики компьютерной информации как предмета), и/или негативными признаками (суждениями, почему та или иная информация не может быть оценена как предмет) в рамках определенного состава преступления.

Рассмотрим общее определение компьютерной информации. В уголовном законодательстве используются термины и выражения разного вида, в частности, общеупотребительные, юридические и технические[10]. Как составной термин «компьютерная информация» не может быть целиком отнесен к одному классу. Он опирается на весьма развитое общеупотребимое понятие «информация»[11], применение которого, однако, в правовой деятельности, как правило, сопровождается отсылкой к его легальному определению в ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации». Специальное значение употребленного в УК РФ термина «информация» подчеркивается данным к нему определением «компьютерная». Таким образом, компьютерная информация, о которой идет речь в ст. 273 УК РФ — это разновидность информации, защищаемой специальными нормами уголовного закона от определенных воздействий и определенных последствий воздействия.

Существенна техническая составляющая понятия компьютерной информации. Ранее, как отмечалось, она связывалась с определенными средствами ее хранения, обработки и передачи — машинными носителями, электронно-вычислительными машинами (ЭВМ), системами ЭВМ или их сетями. Но правовое регулирование сфер быстрого технического и технологического развития, к числу которых относятся и области использования компьютерной информации, не должно отставать от самих инноваций. В настоящее время достаточно широко распространены компьютерные программы прикладного и вспомогательного характера, без которых не могут функционировать многие технические средства. Поэтому появилось указание на квалификацию компьютерной информации независимо от средств ее хранения, обработки и передачи. Сфера действия статьи расширилась и имеет тенденцию к дальнейшему расширению[12].

Законодатель пошел по пути, избранному Конвенцией о преступности в сфере компьютерной информации (Будапешт, 23 ноября 2001 г.), в которой акцент сделан на форме представления информации. По нормам Конвенции, предмет определяемых ею посягательств образует информация в форме, доступной восприятию ЭВМ или передающаяся по каналам связи. В каком виде ЭВМ и иные технические средства могут воспринимать компьютерную информацию? Представление компьютерной информации осуществля-

---

[10] См.: *Иванчин А.В.* Законодательная техника в механизме уголовного правотворчества: учеб. пособие. Ярославль: ЯрГУ, 2009. С. 129.

[11] Информация в переводе с латинского означает «разъяснение», «осведомление», «изложение», «набор сведений», «сообщение». См.: Современный толковый словарь русского языка / гл. ред. С.А. Кузнецов. СПб.: Норинт, 2006. С. 248.

[12] Судебная практика (по делам были проведены экспертизы) обнаруживает вредоносную компьютерную информацию в электронных блоках банкоматов (уголовное дело № 1-553/2009. Приморский районный суд. Цит. по: *Алексанов А.К., Доронин А.М., Демчев И.А. и др.* Безопасность карточного бизнеса. М.: Бизнес-энциклопедия МФПА, 2011), ресиверов (уголовное дело № 1-153/2014. Элистинский городской суд Республики Калмыкия // URL:http://rospravosudie.com (дата обращения: 14 ноября 2014 г.)) и других устройств.

ется с помощью языка, содержащего всего два символа алфавита — 0 и 1. Инженеров такой способ представления информации привлек простотой технической реализации проблемы кодирования. Легко различимые состояния — есть электрический сигнал (1) или нет сигнала (0) позволяют разными способами двоичного кодирования и декодирования, в основе которых лежат логика и математика, распознать и обработать техническими средствами для достижения поставленной задачи любые сведения (сообщения, данные).

Чтобы охватить все объекты информационной среды, субстанционально выраженные способами двоичного кодирования и декодирования, российский законодатель указывает электрические сигналы как форму существования компьютерной информации. Наряду с положительной оценкой это решение вызвало критические замечания. Так, А.В. Суслопаров пишет, что выражение «электрические сигналы» невозможно найти в действующем законодательстве, оно практически не употребляется в литературе, посвященной компьютерным преступлениям, редко встречается в работах, посвященных информации и информационным технологиям[13]. В. Быков и В. Черкасов слабость определения компьютерной информации видят в том, что в сфере информационных технологий возникают все новые нетривиальные пути развития; в технологии, где устройства перестают быть электронными, само понятие «электрический сигнал» может потерять смысл[14].

Научный и технический поиск новых путей и способов представления компьютерной информации может поколебать монополию «электрической» формы ее существования. Имеются сообщения о все более широком применении микросхем MRAM (magnetoresistive random access memory — магниторезистивная память с произвольным доступом). Данные в MRAM записываются не с помощью электрических зарядов, а с помощью магнитной поляризации элементов памяти, что обеспечивает важное для этого типа памяти свойство — возможность сохранять записанные в ячейки данные даже в случае отключения питания[15]. Но пока законодательная дефиниция адекватна отражаемой ею действительности. Тем самым она оказывает благотворное влияние на правоприменительную деятельность[16].

Наше внимание привлекло другое обстоятельство. В судебной практике по ст. 273 УК РФ анализируемое определение компьютерной информации редко является прямым аргументом, т.е. редко используется в качестве обоснования принимаемых выводов. По поводу оценки полезности анализируемого определения можно заметить, что:

• нормативное закрепление общего понятия компьютерной информации корреспондирует факту выделения в УК РФ самостоятельной главы о преступлениях, совершаемых в данной среде. Это усиливает гарантийную функцию уголовного закона в условиях тотального вторжения компьютерной информации в жизнь общества, каждого человека;

---

[13] См.: *Суслопаров А.В.* Указ. соч. // СПС «Гарант».

[14] См.: *Быков В., Черкасов В.* Понятие компьютерной информации как объекта преступлений // Законность. 2013. № 12 // СПС «Гарант».

[15] URL:http://www/top.rbc.ru/economics/19/08/2014/943629.shtml (дата обращения: 14 ноября 2014 г.).

[16] См.: *Кругликов Л.Л.* Дефиниция хищения в уголовном законодательстве Российской Федерации // Законодательная дефиниция: логико-гносеологические, политико-юридические, морально-психологические и практические проблемы: матер. Международного круглого стола (Черновцы, 21–23 сентября 2006 г.). Н.Новгород: НИПРЦ «Юридическая техника», 2007. С. 1114.

• сфера действия исследуемого определения расширяется. Так, в ст. 159.6 УК РФ по признаку использования компьютерной информации выделен один из специальных видов мошенничества. С использованием или в отношении компьютерной информации, понимаемой аналогично, могут совершаться многие другие преступления (ст. 141, 171.2, 185[3], 242 УК РФ и др.). Это обстоятельство преимущественно отражается за счет упоминания о среде существования компьютерной информации — электронных и информационно-телекоммуникационных сетях.

На редкое прямое использование анализируемого предписания при принятии уголовно-правовых решений, очевидно, влияет тот факт, что отдельные статьи УК РФ, по сути, вводят специальное содержание в понятие компьютерной информации в контексте формулируемого запрета. Так, диспозиция ст. 273 УК РФ указывает на совершение действий не вообще с компьютерной информацией, а с компьютерной программой или иной компьютерной информацией, которая:

• заведомо предназначена для уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации ее средств защиты. УК РФ указывает, что компьютерная программа или иная компьютерная информация должны быть вредоносными, т.е. иметь определенное назначение и отвечать этому назначению;

• при условии, что на такое использование компьютерной информации отсутствует санкция (согласие владельца информации).

Для описания в приговоре вида и индивидуальных характеристик такого предмета преступления будет необходимым, например, следующее указание: «программа «x–forse_2012_x52», на жестком диске, заведомо предназначенная для нейтрализации средств защиты компьютерной информации». Применение ст. 146 УК РФ вообще не требует обращения к уголовно-правовому понятию компьютерной информации, поскольку характеристики компьютерных программ как объекта авторского права и предмета данного преступления определены в гражданском законодательстве (ст. 1261 ГК РФ)[17].

Итак, уголовно-правовая оценка компьютерной информации как предмета преступного посягательства, предусмотренного ст. 273 УК РФ, требует учета особенностей такой информации, связанных с особенностями данного состава. Несмотря на формальный состав, законодатель связал в нем наступление ответственности с созданием опасности для той компьютерной информации и средств ее защиты, которые подвергнутся «атаке». В отличие от конкретной опасности (угрозы), когда акцент делается на предметной стороне ситуации, на реальной возможности сейчас причинить вред конкретному объекту, здесь при уголовно-правовой оценке учитывается субъективные признаки: намерение создать и использовать причиняющий потенциал. Его реализация, т.е. фактические изменения в объекте охраны или создание ситуации повышенной вероятности наступления определенных последствий, не требуется. Показательно, однако, что, как было отмечено, применяется рассматриваемая статья исключительно после совершения деяния, как правило, связанного с нейтрализацией средств защиты авторского права на устанавливаемые компьютерные программы.

[17] См.: *Козубенко Ю.В.* Защита авторских прав на программы для ЭВМ в уголовном, административном и гражданском судопроизводстве. М.: Волтерс Клувер, 2009 // СПС «Гарант»; п. 4 Постановления Пленума Верховного Суда Российской Федерации от 26 апреля 2007 г. № 14 «О практике рассмотрения судами уголовных дел о нарушении авторских, смежных, изобретательских и патентных прав, а также о незаконном использовании товарного знака» // Бюллетень Верховного Суда Российской Федерации. 2007. № 7.

В связи с тем, что назначение и способность уничтожить, блокировать, модифицировать, копировать информацию вполне могут быть в определенных сочетаниях и для определенных ситуаций функциями легальных программ, для признания компьютерной информации вредоносной важно установить содержание и значение признака ее предполагаемого несанкционированного действия. Как полагает С.А. Пашин, речь идет: а) об отсутствии предварительного уведомления нового обладателя компьютерной информации о характере ее действия; б) неполучении его согласия на реализацию программой или иной компьютерной информацией своего назначения[18]. Должны быть признаки игнорирования или преодоления воли обладателя информации, т.е. того, что иногда обозначается как «вопреки воле»[19].

Введение этого признака существенно по ряду причин. Во-первых, известны попытки использования «альтернативного» программного обеспечения для борьбы с нарушением авторских прав. В первой половине 90-х годов XX в. вместо создания эффективно действующих правовых механизмов реализации прав многие крупные правообладатели в русле идеи «ответ машине заключается в машине» настаивали, в том числе, на возможности использования для пресечения нарушений и защиты своих прав звукозаписывающими компаниями следующих вариантов программного обеспечения:

- троянов, перенаправляющих пользователей на веб-сайты, где те могут законным образом купить песню или фильм, которые пытались загрузить незаконно;
- программ, блокирующих компьютер на некоторое время и выводящих на экран предупреждение о скачивании пиратских файлов;
- «молчаливого» программного обеспечения, сканирующего жесткий диск и предпринимающего попытки удалить с него любые пиратские файлы;
- «запрещающего» программного обеспечения, блокирующего доступ в Интернет при попытке загрузить пиратские файлы[20].

Подобные меры не включены в число принятых для борьбы с нарушениями авторских прав. Во-первых, в силу законодательного запрета в ст. 273 УК РФ создания, распространения или использования компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, компьютерной информации, они оказываются противозаконными. Во-вторых, понятие санкции не следует связывать с наличием или отсутствием только индивидуальной воли (индивидуального согласия). Усиление контроля за Интернетом и другими информационными сетями означает возможность для государственной власти вторгнуться в информационную среду с помощью специального программного обеспечения (специальных программ копирования для контроля содержания сайтов, выявления и блокирования запрещенной к распространению информации)[21]. Основания такого вторжения, порядок его осуществления должны строго определяться правом и установленными им санкциями-разрешениями.

---

[18] См.: Комментарий к Уголовному кодексу Российской Федерации / под общ. ред. В.М. Лебедева, Ю.И. Скуратова. М.: Норма, 2001. С. 704 (авт. гл. — С.А. Пашин).

[19] См.: Уголовный кодекс Российской Федерации: Постатейный комментарий / науч. ред. Н.Ф. Кузнецова, Г.М. Миньковский. М.: ЗЕРЦАЛО, ТЕИС, 1997. С. 585 (авт. гл. — В.С. Комиссаров).

[20] См.: *Курбалийя Й., Гэлбстайн Э.* Управление Интернетом. Проблемы, субъекты, преграды. М.: МГИМО (У) МИД России, 2005. С. 105–106. Попытки обращения к подобным мерам нельзя исключить и в дальнейшем.

[21] При выполнении оперативно-розыскных мероприятий, пишут Н.Г. Лабутин и С.И. Кувычков, весьма эффективно использовать специальные программные средства сканирования и перехвата тра-

Итак, компьютерная информация как предмет предусмотренного в ст. 273 УК РФ преступления обладает следующим набором признаков: а) это сведения, сообщения, данные; б) представленные в форме электрических сигналов; в) независимо от средств их хранения, обработки и передачи; г) в виде компьютерной программы либо иной (в литературе обычно не расшифровываемой) компьютерной информации; д) заведомо предназначенных для уничтожения, блокирования, модификации, копирования компьютерной информации либо средств защиты компьютерной информации; ж) когда на такое использование компьютерной информации отсутствует необходимая санкция. При отсутствии хотя бы одного из выделенных признаков действия по созданию, использованию или распространению компьютерной информации нельзя рассматривать как преступление, ответственность за которое предусмотрена ст. 273 УК РФ. Например, не отвечает признакам вредоносности предмета программа, использование которой вызывает уничтожение, блокирование и другие последствия лишь в качестве побочного эффекта ее нецелевого использования.

Рассмотренные в статье вопросы определения компьютерной информации как предмета преступления, предусмотренного ст. 273 УК РФ, показывают, что хотя закон имеет дело с одним из символов цифрового мира, здесь нельзя применять цифровую (двоичную) логику «да (хорошо) — нет (плохо)». Тонкости значений использованных понятий требуют учета в правовом регулировании возможного спектра их вариантов. Решение поставленных и иных вопросов, в том числе о практическом значении отдельных признаков компьютерной информации, о применении нормы ст. 273 УК РФ в совокупности со статьями, обеспечивающими безопасность компьютерной информации финансовых систем, информации, составляющей коммерческую тайну, тайну частной жизни, несомненно, требует продолжения дискуссии.

Библиография

Алексанов А.К., Доронин А.М., Демчев И.А. и др. Безопасность карточного бизнеса. М.: Бизнес-энциклопедия МФПА, 2011 // СПС «Гарант».

Быков В., Черкасов В. Понятие компьютерной информации как объекта преступлений // Законность. 2013. № 12 // СПС «Гарант».

Дворецкий М., Копырюлин А. Проблемы квалификации преступлений, сопряженных с созданием, использованием и распространением вредоносных программ // Уголовное право. 2007. № 4. С. 29–33.

Додонов В.Н., Капинус О.С., Щерба С.П. Сравнительное уголовное право. Особенная часть: монография / под общ. ред. С.П. Щербы. М.: Юрлитинформ, 2010. С. 386–392.

Иванчин А.В. Законодательная техника в механизме уголовного правотворчества: учеб. пособие. Ярославль: ЯрГУ, 2009.

Козубенко Ю.В. Защита авторских прав на программы для ЭВМ в уголовном, административном и гражданском судопроизводстве. М.: Волтерс Клувер, 2009 // СПС «Гарант».

фика, передаваемого по компьютерным сетям, связанным с интересующим объектом. Такие программы подразделяются на сканеры Сети и так называемые снифферы, по основному своему предназначению являющиеся инструментами скрытой компьютерной разведки, или «хакерскими» инструментами. См.: *Лабутин Н.Г., Кувычков С.И.* Применение специальных программных средств поиска информации при выявлении преступлений, связанных с легализацией преступных доходов // Легализация преступных доходов как угроза экономической безопасности России: теория, практика, техника гармонизации международно-правовых и национальных механизмов противодействия: сб. ст. / под ред. В.М. Баранова. Н.Новгород: Нижегородская академия МВД России, 2009. С. 787.

Комментарий к Уголовному кодексу Российской Федерации / под общ. ред. В.М. Лебедева, Ю.И. Скуратова. М.: Норма, 2001 (авт. гл. — С.А. Пашин). С. 694–706.

Кругликов Л.Л. Дефиниция хищения в уголовном законодательстве Российской Федерации // Законодательная дефиниция: логико-гносеологические, политико-юридические, морально-психологические и практические проблемы: матер. Международного круглого стола (Черновцы, 21–23 сентября 2006 г.). Н.Новгород: НИПРЦ «Юридическая техника», 2007. С. 1114–1124.

Курбалийя Й., Гэлбстайн Э. Управление интернетом. Проблемы, субъекты, преграды. М.: МГИМО (У) МИД России, 2005.

Лабутин Н.Г., Кувычков С.И. Применение специальных программных средств поиска информации при выявлении преступлений, связанных с легализацией преступных доходов // Легализация преступных доходов как угроза экономической безопасности России: теория, практика, техника гармонизации международно-правовых и национальных механизмов противодействия: сб. ст. / под ред. В.М. Баранова. Н.Новгород: Нижегородская академия МВД России, 2009. С. 784–799.

Современный толковый словарь русского языка / гл. ред. С.А. Кузнецов. СПб.: Норинт, 2006.

Суслопаров А.В. Эволюция института ответственности за компьютерные преступления // Эволюция государственных и правовых институтов в условиях развития информационного общества / отв. ред. И.Л. Бачило. М.: ИГП РАН, Юркомпани, 2012 // СПС «Гарант».

Уголовный кодекс Российской Федерации: Постатейный комментарий / науч. ред. Н.Ф. Кузнецова, Г.М. Миньковский. М.: ЗЕРЦАЛО, ТЕИС, 1997 (авт. гл. — В.С. Комиссаров). С. 580–587.

Computer Information as a Crime under Article 273 of the RF Criminal Code

Artur Engelgardt

Associate Professor of the Department of Criminal Law, Law Faculty, National Research University Higher School of Economics, Candidate of Legal Sciences. Address: 20 Myasnitskaya Str., 101000, Moscow, Russian Federation. E-mail: aengelgardt@hse.ru

Abstract

The position of criminal law as to using and spreading harmful software (information) (article 273 of RF Criminal Code) is a requisite of protecting one of the key principles of regulating information. A specific legislation defines this principle as a freedom of search, using, obtaining, transferring, making and spreading information by any legal means. Facts show that intended balanced and based on the consent understanding of the meaning of the ban under article 273 of RF Criminal Code and other acts (articles 141, 171.2, 185.3, 242, 272 thereof) if they are committed by intruding into the operation of computer or information telecommunication nets depends on the understanding of computer information as the element of the crime in question. This interpretation goes beyond the competence of an expert in criminal law. Thus, the examination of computer information is relevant not only to linguistic purism added to the research of computer crimes. This issue should get a comprehensive study in legal literature and from different angles. The paper shows that the conceptual characteristics of computer information in RF Criminal Code is constantly expanding. First, it is defined commonly as data (information) provided as electric signals available for electronic devices including the transmission by data link channels. Under the obtained empirical material, this definition of computer information is not a corollary from the argument for the opinions and decisions of courts. Its role is different as it does not identify computer information with the means of storing, processing and transferring, find it in various technical devices such as cashpoints, receivers etc. The research shows that in certain articles of the Criminal Code, computer information includes the provisions as to special characteristics (positive signs) and reasons why some information cannot be considered as a subject of crime in question (negative signs). Thus, secondly, computer information as an element of a certain crime has a number of individual signs. Article 273 of RF Criminal Code represent it as 1) a software or other information, b)which is intended for eliminating, blocking, modifying, copying computer information or neutralizing the means of its protection, c) when a necessary

sanction is missing. Some of the abovementioned signs have not had proper examination. In particular, the sign that computer information targets the neutralization of the protection means. In the conditions of common usage of relevant technological instruments, the introduction of this sign has broadened the coverage of article 273 of RF Criminal Code and led to its primitive interpretation.

Keywords

Crime, criminal liability, target of crime, computer information, harmful computer software, neutralizing the means of computer information protection.

Citation: Engelgardt A.A. Computer Information as a Crime under Article 273 of Criminal Code of the Russian Federation. *Pravo. Zhurnal Vysshey shkoly ekonomiki*, no 4, pp. 136–145 (in Russian)

References

Aleksanov A.K., Doronin A.M., Demchev I.A. (2011) Bezopasnost' kartochnogo biznesa [Security of Gambling Business]. Moscow: Biznes-entsiklopediya MFPA.

Bykov V., Cherkasov V. (2013) Ponyatie komp'yuternoy informatsii kak ob"ekta prestupleniy [Concept of Computer Information as a Target of Crime]. Zakonnost', no 12.

Dvoretskiy M., Kopyryulin A. (2007) Problemy kvalifikatsii prestupleniy, sopryazhennykh s sozdaniem, ispol'zovaniem i rasprostraneniem vredonosnykh programm [Problems of Qualifying Crimes Relating to the Creation, Use and Spread of Harmful Software]. Ugolovnoe pravo, no 4, pp. 29–33.

Dodonov V.N., Kapinus O.S., Shcherba S.P. (2010) Sravnitel'noe ugolovnoe pravo. Osobennaya chast': Monografiya [Comparative Criminal Law. Special Part. Monograph]. Moscow: Yurlitinform, pp. 386–392.

Ivanchin A.V. (2009) Zakonodatel'naya tekhnika v mekhanizme ugolovnogo pravotvorchestva: uchebnoe posobie [Legislative Technique in the Mechanism of Criminal Lawmaking. Textbook]. Yaroslavl': YarGU (in Russian)

Kozubenko Yu.V. (2009) Zashchita avtorskikh prav na programmy dlya EVM v ugolovnom, administrativnom i grazhdanskom sudoproizvodstve [Copyright Protection of Software in Criminal, Administrative and Civil Proceedings]. Moscow: Volters Kluver. (in Russian)

Lebedev V.M., Skuratov Yu.I. (Eds.) (2001) Kommentariy k Ugolovnomu kodeksu Rossiyskoy Federatsii [Commentaries to RF Criminal Code]. Moscow: Norma. (in Russian)

Kruglikov L.L. (2007) Definitsiya khishcheniya v ugolovnom zakonodatel'stve RF [Definition of Embezzlement in Criminal Law]. Proceedings of International Panel: Zakonodatel'naya definitsiya: logiko-gnoseologicheskie, politiko-yuridicheskie, moral'no-psikhologicheskie i prakticheskie problem, Chernovtsy, September 21–23, 2006, pp. 1114–1124.

Kurbaliyya Y., Gelbstayn E. (2005) Upravlenie internetom. Problemy, sub"ekty, pregrady [Regulation of The Internet. Problems, Subjects, Barriers]. Moscow: MGIMO (U) MID Rossii. (in Russian)

Labutin N.G., Kuvychkov S.I. (2009) Primenenie spetsial'nykh programmnykh sredstv poiska informatsii pri vyyavlenii prestupleniy, svyazannykh s legalizatsiey prestupnykh dokhodov [Applying Special Search Software to Reveal Crimes]. Legalizatsiya prestupnykh dokhodov kak ugroza ekonomicheskoy bezopasnosti Rossii: teoriya, praktika, tekhnika garmonizatsii mezhdunarodno-pravovykh i natsional'nykh mekhanizmov protivodeystviya: Sbornik statey. Pod red. V.M. Baranova. [Legalizing Criminal Proceeds as a Threat to the Economic Security of Russia: Theory, Practice, Tecnique of Harmonising International and National Mechanisms of Counteracting. V.M. Baranov (ed.)]. Nizhniy Novgorod: Nizhegorodskaya akademiya MVD Rossii, pp. 784–799.

Kuznetsov S.A. (Ed.) (2006) Sovremennyy tolkovyy slovar' russkogo yazyka [Modern Explanatory Dictionary of the Russian Language]. Saint Petersburg: Norint. (in Russian)

Susloparov A.V. (2012) Evolyutsiya instituta otvetstvennosti za komp'yuternye prestupleniya [The Evolution of the Institute of Liability for Computer Crimes]. Evolyutsiya gosudarstvennykh i pravovykh institutov v usloviyakh razvitiya informatsionnogo obshchestva / Otv. red. I.L. Bachilo [Evolution of State and Legal Institutions during the Development of Information Society. Bachilo I.L. (ed.)]. Moscow: IGP RAN, Yurkompani.

Kuznetsova N.F., Min'kovskiy G.M. (Eds.) (1997) Ugolovnyy kodeks Rossiyskoy Federatsii: Postateynyy kommentariy [Criminal Code of the Russian Federation. Commentaries. Moscow: Zertsalo, TEIS. (in Russian)