СТАТЬЯ 274 УГОЛОВНОГО КОДЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ: НОВАЯ РЕДАКЦИЯ - СТАРЫЕ ПРОБЛЕМЫ

THE ARTICLE 274 OF THE CRIMINAL CODE OF RUSSIAN FEDERATION: NEW VERSION - OLD PROBLEMS

M. Efremova

Annotation

This article examines the updated version of article 274 of the Criminal code of Russian Federation. The author notes that the previous legal structure of article 274 was not entirely successful, making it difficult to use.However, despite the legislation changes, this problem was not solved. Pointing out shortcomings of the new wording of article 274 of the criminal code, the author makes suggestions for improving the existing criminal law.

Keywords: computer information, computer information and telecommunications network, crimes in the sphere of computer information.

Ефремова Марина Александровна
К.ю.н., доцент,
Ульяновский государственный университет

Аннотация

В статье исследуется обновленная редакция статья 274 Уголовного кодекса Российской Федерации. Автором отмечается, что прежняя законодательная конструкция ст. 274 была не совсем удачной, что затрудняло ее применение. Однако, не смотря на внесенные законодателем изменения, данная проблема не решилась. Указывая на выявленные недостатки новой редакции ст. 274 УК РФ, автор высказывает предложения по совершенствованию действующего уголовного законодательства.

Ключевые слова:

Компьютерная информация, компьютер, информационно-телекоммуникационная сеть, преступления в сфере компьютерной информации.

В последнее время появились новые вызовы и угрозы национальной безопасности России, которые нашли отражение в новой Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 31.12.2015 г. №683.Так, в Стратегии подчеркивается, что все большее влияние на характер международной обстановки оказывает усиливающееся противоборство в глобальном информационном пространстве, обусловленное стремлением некоторых стран использовать информационные и коммуникационные технологии для достижения своих геополитических целей, в том числе путем манипулирования общественным сознанием и фальсификации истории. Появляются новые формы противоправной деятельности, в частности с использованием информационных, коммуникационных и высоких технологий. Среди главных направлений обеспечения государственной и общественной безопасности в Стратегии говорится о совершенствовании правового регулирования предупреждения преступности, в том числе в информационной сфере.

Уголовный кодекс Российской Федерации содержит главу 28 "Преступления в сфере компьютерной информации", которая как раз и служит этой цели. Среди трех ее статей наибольшие споры у ученых вызывает ст. 274 "Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей". Необходимо отметить, что Федеральным законом от 07.12.2011 № 420-ФЗ в нее были внесены изменения – статья получила новую редакцию. Вместе с тем обе редакции статьи характеризуются тем, что она носит бланкетный характер. Это означает, что при квалификации содеянного необходимо точное установление того правила, которое было нарушено. Во многом именно по указанной причине возникают сложности в правоприменительной практике. В период действия прежней редакции ст. 274 УК РФ таковая и вовсе отсутствовала из-за недостатков законодательной конструкции анализируемого состава. В этой связи многие авторы высказывались о необходимости исключения ее из УК РФ.

Объектом преступления, предусмотренного ст. 274 УК РФ выступают отношения, обеспечивающие безопасность в сфере эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Предметом преступления, предусмотренного ст. 274 УК РФ, являются средства хранения, обработки или передачи компьютерной информации, информационно-телекоммуникационные сети и оконечное оборудование. Законодатель отказался от терминов ЭВМ, система ЭВМ, сеть ЭВМ, используемых в предыдущей редакции

По мнению А.Н. Ягудина, предложенный законодателем вместо "ЭВМ" термин "средства хранения, обработки

или передачи охраняемой компьютерной информации" не выдерживает критики. Он полагает, что под средством хранения компьютерной информации можно понимать и ящик стола, и картонную коробку, где люди обычно хранят электронные носители компьютерной информации, такие как DVD и CD–диски, карты памяти и прочее [5].

Не соглашаясь с данной позицией, отметим, что с развитием научно–технического прогресса компьютерная информация может обращаться и храниться в различных технических устройствах, в том числе смартфонах, планшетных компьютерах. Поэтому отказ законодателя от термина "ЭВМ" вполне закономерен и обусловлен объективными факторами. Средствами хранения, обработки или передачи компьютерной информации следует считать не только компьютеры, а любые устройства, на которых зафиксирована или в которых обращается компьютерная информация.

Под информационно–телекоммуникационной сетью, в соответствии с Федеральным законом "Об информации, информационных технологиях и защите информации"понимается технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. Под оконечным оборудованием понимается оборудование, преобразующее информацию в данные для передачи по линии связи и осуществляющее обратное преобразование.

Понятие оконечного оборудования дается в Федеральном законе "О связи", где под таковым понимаются технические средства для передачи и (или) приема сигналов электросвязи по линиям связи, подключенные к абонентским линиям и находящиеся в пользовании абонентов или предназначенные для таких целей.

Объективная сторона анализируемого преступления характеризуется как действием, так и бездействием. По справедливому утверждению Ю.М. Батурина и С.В. Полубинской, к правилам, нарушение которых входит в объективную сторону данного состава преступления, не относятся те, которые ограничивают доступ к охраняемой законом компьютерной информации [1]. В последнем случае деяние следует квалифицировать по ст.272 УК РФ. В любом случае при привлечении субъекта к ответственности приходится обращаться к характеристике тех требований, прав и обязанностей, которые лицо нарушило. Необходимо отметить, что подобных правил в настоящее время существует великое множество. Поэтому в науке по данному вопросу развернулась дискуссия.

Так, по мнению одних авторов, под правилами эксплуатации глобальных сетей понимаются нормативные акты, регламентирующие работу данной сети, в частности, Федеральный закон "О связи", регламентирующий порядок создания и подключения к информационно–телекоммуникационной сети Интернет. Примерами иных нормативных актов, устанавливающих правила эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно–телекоммуникационных сетей, могут служить: во–первых, общероссийские правила, например, Временные санитарные нормы и правила для работников вычислительных центров; во–вторых, техническая документация на компьютерную технику; в–третьих, конкретные принимаемые в определенном учреждении или организации оформленные нормативно и доведенные до сведения соответствующих работников инструкции и правила внутреннего порядка, например, Положение об обеспечении безопасности информации в Государственной автоматизированной системе Российской Федерации "Выборы", утвержденное Постановлением Центральной избирательной комиссии РФ от 23.07.2003 З 19/137–4 [4].

Другие же под правилами использования компьютерной техники или ее сети понимает правила, установленные федеральным законом, изготовителем или организацией, учреждением либо государственным органом, предоставившим доступ к компьютерной технике или ее сети определенному кругу пользователей [5].

Действительно, в настоящее время отсутствуют специальные единые правила эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно–телекоммуникационных сетей. В этой связи приходится обращаться к отдельным положениям федеральных законов, регулирующих эту сферу, а так же к подзаконным нормативным актам, государственным стандартам, локальным нормативным актам.Кроме того, в настоящее время по смыслу данной статьи, лицо можно привлечь к уголовной ответственности за несоблюдение требований, указанных в руководстве пользователя, прилагаемого к компьютеру или его составляющим, либо же программным продуктам. По нашему мнению, несоблюдение требований, к примеру, ГОСТ, а тем более инструкции по эксплуатации компьютера, не может выступать основанием привлечения к уголовной ответственности.

Нарушение правил эксплуатации может быть осуществлено путем как активного действия, (например, использование служебных аппаратных и программных средств в личных целях), так и бездействия, (например, не проведение обязательного резервного копирования базы данных). По мнению М.В. Дворецкого, объективная сторона данного преступления может выражаться в несвоевременном техническом обслуживании узлов и агрегатов; в неправильном подключении компьютера к источникам питания; в отказе от использования антивирусного программного обеспечения, паролей и иных средств защиты и т.д. [2].

В качестве обязательного признака статья 274 предусматривает наступление общественно–опасных последствий: во–первых, нарушение специальных правил должно повлечь уничтожение, блокирование или модификацию охраняемой законом компьютерной информации, во–вторых, уничтожение, блокирование или модификация информации должны причинить крупный ущерб (ущерб, сумма которого превышает один миллион рублей). А.Н. Ягудин предлагает исключить указанные по–

следствия из диспозиции ст. 274 УК РФ и квалифицировать деяние, повлекшее такие последствия, по ст. 272 УК РФ [5]. Что же касается крупного ущерба, как одного из последствий рассматриваемого деяния, то необходимо отметить, что в предыдущей редакции рассматриваемой статьи использовалась оценочная категория "существенный вред". Совершенно справедливо, что законодатель отказался от нее.

Не являются преступлением, предусмотренным статьей 274, умышленные действия, повлекшие уничтожение, блокирование информации путем нарушения целостности средств хранения, обработки или передачи компьютерной информации и информационно–телекоммуникационных сетей, в частности хищение отдельных составных устройств, повреждение или уничтожение оборудования.В таких случаяхдеяния должны квалифицироваться по соответствующим статьям главы 21 УК РФ.

С субъективной стороны деяние может характеризоваться виной как в форме умысла (чаще – косвенного), так и в форме неосторожности.

Субъект данного преступления – специальный. Это лицо, которое в силу должностных обязанностей имеет доступ к средствам хранения, обработки или передачи охраняемой компьютерной информации либо информационно–телекоммуникационным сетям и оконечному оборудованию, а также к информационно–телекоммуникационным сетям. Однако, на наш взгляд, основным условием привлечения лица к ответственности должна быть не возможность доступа к средствам хранения, обработки или передачи охраняемой компьютерной информации либо информационно–телекоммуникационным сетям и оконечному оборудованию в силу должностных обязанностей, а таковой должна выступать обязанность соблюдать установленные правила обращения со средствами хранения, обработки или передачи компьютерной информации либо информационно–телекоммуникационными сетями и оконечным оборудованием. Если же на лицо должностными или иными инструкциями, специальными актами такая обязанность не возложена, то оно не должно подлежать уголовной ответственности.

Ч. 2 ст. 274 УК РФ предусматривает ответственность за то же деяние, если оно повлекло тяжкие последствия или создало угрозу их наступления.

Как отмечает О.К. Зателепин, понятие "тяжкие последствия" включает в себя все возможные виды вреда, а именно материальный (физический и имущественный), организационный, экологический и т. д. Для уяснения содержания термина "тяжкие последствия" в той или иной статье уголовного законодательства необходимо установить взаимосвязь с объектом уголовно–правовой охраны[3]. Применительно к рассматриваемому составу преступления, объектом которого, как уже было отмечено, выступают отношения, обеспечивающие безопасность в сфере эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно–телекоммуникационных сетей, можно предположить, что должны в себя включать эти последствия. Полагаем, что к ним можно отнести остановку производства на предприятиях, если им управляет компьютер; остановку работы аэропортов, ресурсоснабжающих организаций и т.д.

Проведенный анализ наглядно демонстрирует, что с момента своего принятия, данная статья обречена на неприменение. Она переняла все "больные места" предыдущей редакции, хотя, казалось бы, должна была их устранить. Пока отсутствуют специальные единые правила эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно–телекоммуникационных сетей, закрепленные законодательно на федеральном уровне, следует обращаться к положением ГОСТ, СанПиН, локальных актов учреждений и организаций. Однако их нарушение должно влечь никак не уголовную, а дисциплинарную ответственность, учитывая, что наиболее строгое наказание, которое предусмотрено ч. 1. ст. 274 является лишение свободы на срок до двух лет (а по ч. 2 ст. 274 – до пяти лет), что явно не соответствует общественной опасности данного деяния. Резюмируя вышеизложенное, следует признать ст. 274 УК РФ примером излишней криминализации и исключить из УК РФ.

ЛИТЕРАТУРА

1. Батурин Ю.М., Полубинская С.В. Компьютерные преступления: нормы, правоприменение, оценка // Российский ежегодник уголовного права. 2006. – СПб.: Издательский дом Санкт–Петербургского государственного университета, 2007. С. 139 – 160.

2. Дворецкий М.Ю. Корреляции глава 28 УК РФ в контексте оптимизации уголовной ответственности и повышения эффективности правоприменительной практики // Вестник Тамбовского государственного университета. 2012. вып. 6(110). С. 266 – 271.

3. Зателепин О.К. Объект преступления против военной службы: дис... канд. юрид. наук. – М., 1999. – 211с.

4. Комментарий к Уголовному кодексу Российской Федерации / под.ред. В.М. Лебедева. – М.: Юрайт, 2013. – 1069с.

5. Ягудин А.Н. Уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно–телекоммуникационных сетей: дис. … канд. юрид. наук. – Казань, 2013. – 218с.