УДК 343.34

ПРОБЛЕМА НАЗНАЧЕНИЯ ОТВЕТСТВЕННОСТИ ЗА СОЗДАНИЕ, РАСПРОСТРАНЕНИЕ И ИСПОЛЬЗОВАНИЕ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ

Позднякова Е. Ю.
Студентка юридического факультета, 3 курс
Кубанский государственный Аграрный Университет
Им. И. Т. Трубилина
г. Краснодар, Россия
Медведев С. С.
Доцент к.н., кандидат юридических наук
Кубанский государственный Аграрный Университет
Им. И. Т. Трубилина
г. Краснодар, Россия

THE PROBLEM OF ASSIGNING RESPONSIBILITY FOR THE CREATION, DISTRIBUTION AND USE OF MALICIOUS COMPUTER PROGRAMS

Pozdnyakova E. Yu.
Law student, 3 course
Kuban State Agrarian University
In the name of I.T. Trubilin
Krasnodar, Russia
Medvedev S. S.
Associate Professor Ph.D., Candidate of Law
Kuban State Agrarian University
Name. I.T. Trubilina
Krasnodar, Russia

Аннотация. В данной статье рассматривается проблема, суть которой, на наш взгляд, заключается в декриминализации нормы уголовного закона, связанной с созданием, распространением и использованием вредоносных компьютерных программ. С одной стороны, умышленное нарушение работы компьютера, вследствие чего может быть уничтожена, скопирована, модифицирована, заблокирована конкретная информация, безусловно, является противоправным деянием, но с другой стороны, ответственность за данное деяние слишком сурова, в связи с чем мы предлагаем решение указанной проблемы.

Annotation. This article discusses a problem, the essence of which, in our opinion, is decriminalization of the criminal law norm related to the creation, distribution and use of malicious computer programs. On the one hand, a deliberate disruption of the computer, as a result of which specific information can be destroyed, copied, modified, blocked, is certainly an unlawful act, but on the other hand, the responsibility for this act is too severe, in connection with which we propose a solution to this problem.

Ключевые слова: киберпреступность, вредоносная компьютерная программа, уголовная ответственность, административная ответственность, декриминализация.

Keywords: cybercrime, malicious computer program, criminal liability, administrative responsibility, decriminalization.

В наше время вопросы обеспечения кибербезопасности затрагивают всё мировое сообщество, в том числе и Российскую Федерацию (далее – РФ). Развитие информационных технологий влияет на изменение общественных отношений, касающихся использования компьютерной информации. Согласно пункту 1 примечания к статье 272 Уголовного кодекса РФ [2] под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Таким образом, существует законодательное закрепление указанного понятия, что должно повысить эффективность правоприменения. Следует отметить, что до 2011 года уголовный закон не содержал легального определения компьютерной информации: изменения были внесены Федеральным законом (далее – ФЗ) «О внесении изменений в УК РФ» [5].

Компьютерная информация имеет очень важное значение в жизни каждого отдельно взятого гражданина или юридического лица. Это связано с тем, что сейчас вся информация переносится на электронный носитель в целях

упрощения жизнедеятельности населения. Несомненно, это является плюсом, так как некоторые процессы, которые ранее занимали большой объем по времени, убыстряются. К примеру, с развитием системы портала государственных услуг гражданам не приходится стоять в больших очередях, чтобы, допустим, записаться на прием к врачу: все это можно сделать удаленно, не выходя из дома, воспользовавшись Интернетом. Но есть и минусы такого прогресса.

Развитие компьютерной сферы общественных отношений повлекло за собой появление специалистов в данной области. Негативная сторона такого явления заключается в том, что некоторые такие специалисты используют свои знания в области информационных технологий в противовес требований закона. В связи с этим законодателем принимаются различные нормативные правовые акты, нормы которых направлены на регулирование данной сферы. Иными словами, государство устанавливает рамки дозволенного поведения, ограничивая противоправные действия (бездействие) одних лиц в ущерб интересов других. Так, к примеру, ФЗ «Об информации» [4] закрепляет положение о том, что правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на принципе неприкосновенности частной жизни, недопустимости сбора, хранения, использования и распространения информации о частной жизни лица без его согласия.

Многие лица, получающие доступ к компьютерным системам и сетям, убеждены, что они не делают ничего противозаконного и уголовно наказуемого (а если исходить из действующего уголовного кодекса, то так оно и есть), даже если им приходится нарушать системы защиты, установленные пользователем [1, 94]. Однако для нормального функционирования компьютерных систем и обеспечениябезопасности хранения и передачи информации уголовный закон должен защищать компьютер любого пользователя, пользующегося средствами защиты.

В УК РФ предусмотрено всего 4 состава преступления в сфере компьютерной информации (глава 28). На наш взгляд, ответственность, предусмотренная статьей 273 УК РФ за создание, распространение или использование компьютерных программлибо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информацииявляется слишком суровой за данное деяние. Прежде чем аргументировать необходимость декриминализации указанной нормы, стоит разобраться в понятийном аппарате.

Создание вредоносной программы либо иной компьютерной информации — это результат деятельности, который был представлен в объективной форме определенной системы данных и команд, предназначенных для функционирования информационных сетей, компьютеров, имеющих целью уничтожение, блокирование, модификацию, копирование информации, а также нарушение работы информационных сетей.Использование вредоносных программ — это действия по введению данных программ в оборот. Распространение вредоносных программ — это предоставление неограниченному кругу лиц доступа к указанной программе путем передачи, продажи, проката, предоставления взаймы для любой из этих целей. Таким образом, создание, распространение и использование носят умышленный характер деяния [6, С. 1317].

Мы считаем, что решить обозначенную проблему, суть которой заключается в необходимости декриминализации нормы уголовного закона, можно путем введения преюдициального состава. Необходимо дополнить главу 13 «Административные правонарушения в области связи и информации» Кодекса Российской Федерации об административных правонарушениях (далее – КоАП) [3] статьей 13.41 «Создание, использование и распространение вредоносных компьютерных программ» следующего содержания:

«Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, -

влечет наложение административного штрафа на граждан в размере от двадцати тысяч рублей до пятидесяти тысяч рублей; на должностных лиц – от ста тысяч рублей до двухсот тысяч рублей».

В связи с этим предлагается изменить часть 1 статьи 273 УК РФ и изложить в следующей редакции:

«1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, совершенные лицом, подвергнутым административному наказанию за аналогичное деяние».

Таким образом, проблема назначения ответственности за деяние, предусмотренное частью 1 статьи 273 УК РФ, заключается в необходимости декриминализации указанной нормы уголовного закона. Несмотря на противоправное поведения субъекта преступления, данное деяние, на наш взгляд, не содержит в себе такого уровня общественной опасности, который характерен для преступления. На данный момент применение этой статьи не во всегда является обоснованным. Во многих случаях можно было обойтись применением административной ответственности к виновному. В связи с этим было предложено решение указанной проблемы путем введения преюдициального состава.

Список литературы

1. Бураева Л. А. О некоторых вопросах обеспечения кибербезопасности в современных условиях // Теория и практика общественного развития. 2015. № 13. С. 94;

2. «Уголовный кодекс Российской Федерации» от 13.06.1996 (ред. от 23.04.2019) N 63-ФЗ // СЗРФ № 25 от 17 июня 1996 года, ст. 2954;

3. «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 (ред. от 01.05.2019) N 195-ФЗ // СЗРФ № 1 от 7 января 2002 года, ст. 1;

4. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 18.03.2019) «Об информации, информационных технологиях и о защите информации» // СЗРФ № 31 от 31 июля 2006 года (Части I-II), ст. 3448;

5. Федеральный закон от 07.12.2011 N 420-ФЗ (ред. от 03.07.2016) «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» // СЗРФ № 50 от 12 декабря 2011 года, ст. 7362;

6. Энгельгардт А. А. Уголовно-правовая оценка создания, использования и распространения вредоносных компьютерных программ (информации) // LexRussica. 2014. № 11. С. 1317.