УДК 343.533

Шульга Андрей Владимирович
кандидат юридических наук, доцент,
заведующий кафедрой уголовного права,
Кубанский государственный
аграрный университет имени И.Т. Трубилина
cshulga@rambler.ru
Галиакбаров Ромэн Рахиммулович
доктор юридических наук, профессор,
профессор кафедры уголовного права,
Кубанский государственный
аграрный университет имени И.Т. Трубилина
cshulga@rambler.ru
Andrey V. Shulga
Candidate of Law, Associate Professor,
Head of the Department of Criminal Law,
The Kuban state Agrarian University named after I.T. Trubilina
cshulga@rambler.ru
Romain R. Galiakbarov
Doctor of Law, Professor,
Professor of the Criminal Law Department,
The Kuban state Agrarian University named after I.T. Trubilina
cshulga@rambler.ru

Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1. УК РФ)

Criminal liability for unlawful interference critical information infrastructure The Russian Federation (Article 274.1 of the Criminal Code of the Russian Federation)

Аннотация. *В Уголовный кодекс Российской Федерации в главу О преступлениях в сфере компьютерной информации с 01.01.2018 г. введена статья, предусматривающая ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. В связи с этим возникают вопросы о совершенстве законодательной техники при конструировании данной статьи, а также вопросы регламентации уголовной ответственности при совершении преступления, предусмотренного данной статьей УК РФ.*

Ключевые слова: *преступления в сфере компьютерной информации, посягательство на критическую информационную инфраструктуру РФ, состав преступления, предмет преступления, уголовная ответственность.*

Abstract. *In the Criminal Code of the Russian Federation, a chapter on crimes in the field of computer information has been introduced since 01.01.2018, providing for liability for undue influence on the critical information infrastructure of the Russian Federation. In this regard, there are questions about the perfection of the legislative technique in the construction of this article, as well as the issues of the regulation of criminal responsibility in the commission of a crime provided for in this article of the Criminal Code.*

Keywords: *crimes in the sphere of computer information, encroachment on the critical information infrastructure of the Russian Federation, the creation of a crime, the subject of a crime, criminal responsibility.*

Изучение проблем уголовной ответственности за преступления против компьютерной информации или за преступления, совершенные при помощи компьютерной информации является все более актуальным в науке уголовного права [4, с. 95-155]. В целях совершенствования правоприменительной практики в данной сфере уголовное законодательство нуждается в дальнейшем обновлении, поэтому, в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" права [2, ст. 1], в Уголовный кодекс Российской Федерации права [1, гл. 28] (далее по тексту – УК РФ) Федеральным законом от 26.07.2017 N 194-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации" введена статья 274.1. УК РФ "неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации" права [3, ст.1]. Данная статья вступила в силу с 01.01.2018 г.

Как нам видится, причиной включения статьи 274.1 в УК РФ является приоритет предотвращения компьютерных атак на общественные отношения в сфере обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, то есть, в целях борьбы с компьютерными атаками на информационные ресурсы Российской Федерации.

Исходя из своей конструкции, состав преступления, предусмотренный ст. 274.1 УК РФ, является специальным по отношению к традиционным составам главы 28 УК РФ "Преступления в сфере компьютерной информации", закрепленным в ст.ст. 272-274 УК РФ и выделяется исключительно по специфике предмета преступления в нем закрепленного.

Предметом преступлений, предусмотренных в ст. 274.1 УК РФ, является компьютерная информация, содержащаяся в критической информационной инфраструктуре Российской Федерации (обрабатываемая значимым объектом критической информационной инфраструктуры РФ), либо сама критическая информационная инфраструктура РФ.

Таким образом, диспозиция ст. 274.1 УК РФ является бланкетной. Для установления признаков предмета преступления, предусмотренного ст. 274.1 УК РФ, необходимо ссылаться на вышеупомянутый Федеральный закон “О безопасности критической информационной инфраструктуры Российской Федерации” и установить следующее:

1. В соответствии со ст. 2 Федерального закона “О безопасности критической информационной инфраструктуры Российской Федерации” критическую информационную инфраструктуру образуют: информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, а также сети электросвязи, используемые для организации их взаимодействия.

2. Данные информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, а также сети электросвязи на праве собственности, аренды или на ином законном основании должны принадлежать субъектам критической информационной инфраструктуры - государственным органам, государственным учреждениям, российским юридическим лицам и (или) индивидуальным предпринимателям, которые обеспечивают взаимодействие указанных систем или сетей.

3. Они должны относиться к сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иным сферам финансового рынка, топливно-энергетического комплекса, к области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности.

4. Названные элементы, образующие критическую информационную инфраструктуру, должны быть значимы, то есть, им должна быть присвоена одна из категорий значимости (первая, вторая или третья), и они должны быть включены в реестр значимых объектов критической информационной инфраструктуры.

Реестр значимых объектов критической информационной инфраструктуры ведется федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации. Порядок категорирования объектов критической информационной инфраструктуры регламентируется Федеральным законом “О безопасности критической информационной инфраструктуры Российской Федерации”.

5. Информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления должны относиться к информационным ресурсам РФ, то есть, находиться на территории РФ, в дипломатических представительствах и (или) консульских учреждениях РФ.

Таким образом, для определения предмета преступления, предусмотренного ст. 274.1 УК РФ вышеназванные признаки должны быть установлены в совокупности. Однако изучив эти признаки, которые формулирует специальный нормативный акт, можно утверждать, что они являются в значительной

степени оценочными, определяться должны в каждом конкретном случае следствием и судом.

Например, в соответствии с п. 12 ст. 7 закона “О безопасности критической информационной инфраструктуры РФ” категория значимости, к которой отнесен значимый объект критической информационной инфраструктуры, может быть изменена в порядке, предусмотренном для категорирования.

Таким образом, в процессе квалификации преступления по ст. 274.1 УК РФ возможна ситуация, что предмет указанного преступления утратил свои признаки и необходима переквалификация данного деяния по иным статьям главы 28 УК РФ о преступлениях в сфере компьютерной информации. И такой процесс возможен на любых этапах существования уголовно-правовых отношений: от привлечения к уголовной ответственности до снятия либо погашения судимости. Очевидно, что такая практика не будет способствовать улучшениям в работе правоохранительных органов. Тем более, что исходя из положений п. 12 ст. 7 вышеупомянутого закона, не указано, “в какую сторону” может быть изменена категория значимости указанных объектов – повышения или снижения значимости. И нет никаких препятствий повторять этот процесс изменения значимости несколько раз.

Как мы уже отметили выше, состав преступления, указанный в ст. 274.1 УК РФ, предусматривает ответственность за деяния, обладающие повышенной общественной опасностью по сравнению с деяниями, отраженными в ст.ст. 272-274 УК РФ. И эта разница в общественной опасности должна быть отражена в первую очередь в характеристике санкций указанных составов.

Но судя по сравнению санкций общих и специального состава, эта разница в общественной опасности прослеживается не достаточно четко. Представим это на сравнении наказаний в виде лишения свободы за данные преступления.

Так, санкция преступления, предусмотренного ч. 1 ст. 274.1 УК РФ (специальный состав), предусматривает за его совершение наказание в виде лишения свободы сроком от двух до пяти лет, а санкция тождественного с ним преступления, предусмотренного ч. 1 ст. 273 УК РФ (общий состав), предусматривает за его совершение наказание в виде лишения свободы сроком до четырех лет.

На наш взгляд, такой размер санкции вновь вводимого в УК РФ преступления (даже не изменяющая категорию преступления – как общий, так и специальный состав относятся к одной категории преступлений - средней тяжести) не будет в полной мере свидетельствовать о повышенной общественной опасности деяний, предусмотренных ч. 1 ст. 274 УК РФ. Тем более, что санкция вновь вводимого состава позволяет судам назначать наказание меньшее, чем пять лет лишения свободы.

Недостатком наказания, предусмотренного ч. 3 ст. 274.1 УК РФ – лишение свободы сроком до шести лет, является отсутствие нижнего предела. Смежная общая норма, закрепленная в ч. 1 ст. 274 УК РФ, предусматривает наказание в виде лишения свободы сроком до двух лет лишения свободы. Таким образом, у судов есть возможность назначать и при совершении преступ-

ления, предусмотренного ч. 3 ст. 274.1 УК РФ, также наказание в виде лишения свободы сроком на два года. И тогда стирается всякая грань в оценке уровня общественной опасности при квалификации деяния, как по общему, так и специальному составу преступления против компьютерной информации.

Такая же ситуация может сложиться (суд может назначить равные сроки наказания в виде лишения свободы) и при назначении наказания за данные преступления, совершенные групповым способом (за преступления, предусмотренные ч. 4 ст. 274.1 УК РФ и ч. 3 ст. 272, ч. 2 ст. 273 УК РФ). Так как за преступление, предусмотренное специальной нормой предусмотрено наказание в виде лишения свободы сроком от трех до восьми лет (ч. 4 ст. 274.1 УК РФ), а общей нормой (ч. 3 ст. 272 или ч. 2 ст. 273 УК РФ) – на срок до пяти лет. Например, в чем будет заключаться оценка повышенной общественной опасности компьютерного преступления с учетом специфики его предмета, если за совершение деяния, предусмотренного ч. 4 ст. 274.1 УК РФ, суд назначит, скажем, три, четыре или пять лет лишения свободы?

Аналогичную параллель можно провести и с размерами наказаний, предусмотренных ч. 5 ст. 274.1 УК РФ и ч. 4 ст. 272 УК РФ, ч. 3 ст. 273 УК РФ установленных за совершение компьютерных преступлений, повлекших тяжкие последствия. Часть 5 ст. 274.1 УК РФ предусматривает санкцию в виде лишения свободы сроком от пяти до десяти лет, а ч. 4 ст. 272 УК РФ, ч. 3 ст. 273 УК РФ – до семи лет. В данном случае все названные преступления оцениваются как тяжкие (что снижает дифференциацию их уровня общественной опасности), и за их совершение суд может назначить одинаковые наказания – скажем, пять, шесть или семь лет лишения свободы.

Зачем в таких вышеназванных случаях выделять общие и специальные составы компьютерных преступлений, если они могут повлечь одинаковые наказания и относятся к одинаковой категории преступлений? Поэтому, должно быть более четкое разделение их уровня общественной опасности при помощи законодательно установленных санкций. На наш взгляд, общие и специальные составы должны закреплять преступления, относящиеся к различным категориям (если общий состав закрепляет преступление средней тяжести, то специальный – тяжкое преступление, и т.д.). И верхний предел наказания за совершение преступления, предусмотренного общей нормой, должен быть нижним пределом санкции, закрепленной за совершение преступления, предусмотренного специальной нормой.

В анализируемой нами главе 28 “Компьютерные преступления” примеры применения такого правила оценки уровня общественной опасности есть. Как мы уже указывали, ч. 5 ст. 274.1 УК РФ устанавливает за неправомерное воздействие на критическую информационную инфраструктуру РФ, повлекшее тяжкие последствия, санкцию в виде лишения свободы сроком от пяти до десяти лет, а за аналогичное преступление, предусмотренное ч. 2 ст. 274 УК РФ – до пяти лет лишения свободы. То есть санкция за преступление, предусмотренное специальной нормой, является “продолжением” санкции общей нормы.

Часть 2 ст. 274.1 УК РФ также в этом смысле предусматривает справедливую санкцию - наказание в виде лишения свободы на срок от двух до шести лет (для сравнения, тождественный состав – ч.1 ст. 272 УК РФ предусматривает наказание в виде лишения свободы на срок до двух лет). Тем самым, специальный состав переведен в категорию тяжких преступлений, верхний предел санкции общей нормы является нижним пределом санкции специальной нормы.

Таким образом, выявленные недостатки законодательной техники при построении уголовно-правовой нормы, закрепленной ст. 274.1 УК РФ, должны быть устранены в целях стабилизации судебно-следственной практики.

Литература.

1. Уголовный кодекс РФ от 24 мая 1996 г. // Собрание законодательства. 1996 г. № 25. Ст. 2954.

2. О безопасности критической информационной инфраструктуры Российской Федерации. Федеральный закон от 26.07.2017 N 187-ФЗ // Российская газета № 167 от 31.07.2017.

3. О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации". Федеральный закон от 26.07.2017 N 194-ФЗ // Российская газета № 167 от 31.07.2017.

4. Шульга А.В. Хищения в условиях развития современных информационных технологий и рынка инновационных товаров. М. 2016.

References.

1. The Criminal Code of the Russian Federation of May 24, 1996 // Collection of Legislation. 1996, No. 25. Art. 2954.

2. On the Security of the Critical Information Infrastructure of the Russian Federation. Federal Law of July 26, 2017 N 187-FZ // Rossiyskaya Gazeta No. 167 of July 31, 2017.

3. On Amendments to the Criminal Code of the Russian Federation and Article 151 of the Code of Criminal Procedure of the Russian Federation in connection with the adoption of the Federal Law "On the Security of the Critical Information Infrastructure of the Russian Federation." Federal Law of July 26, 2017 N 194-FZ / / Russian Newspaper No. 167 of July 31, 2017.

4. Shulga A.V. Theft in the conditions of the development of modern information technologies and the market of innovative products. M. 2016.