Vestnik YarGU. Seriya Gumanitarnye nauki. 2023. Vol. 17, No 3
journal homepage: http://j.uniyar.ac.ru/index.php/vyrgu

LAW

Criminal-legal assessment of cyberextortion

I. D. Prudnikov[1]

[1]P. G. Demidov Yaroslavl State University, 14 Sovetskaya str., Yaroslavl 150003, Russian Federation

DOI: 10.18255/1996-5648-2023-3-426-433

Research article
Full text in Russian

The article discusses the issues of qualification of cyberextortion. In particular, this act is analyzed as a kind of ordinary extortion, as well as a kind of exclusively informational crime. It is concluded that in addition to the threats characteristic of article 163 of the Criminal Code of the Russian Federation, there are also threats that are not included in the list of methods of committing a crime listed in this article, and, accordingly, the impossibility of bringing a person to criminal responsibility for a number of variations of cyberextortion under article 163 of the Criminal Code of the Russian Federation. Since it also seems problematic to qualify such acts according to the totality of article 163 and the norms of the Criminal Code of the Russian Federation on crimes in the field of computer information, the author believes that it is necessary to modernize the criminal law and proposes to supplement the disposition of article 163 of the Criminal Code of the Russian Federation with new ways of committing this crime.

Keywords: computer crimes; cyberextortion; ransomwares; cryptocurrencies; criminal law

INFORMATION ABOUT AUTHORS

Prudnikov, Ilya D. | EE-mail: ilya.prudnikov.97@gmail.com
Postgraduate

Вестник ЯрГУ. Серия Гуманитарные науки. 2023. Том 17, № 3
веб-сайт: http://j.uniyar.ac.ru/index.php/vyrgu

Уголовно-правовая оценка кибервымогательства

И. Д. Прудников[1]

[1]Ярославский государственный университет им. П. Г. Демидова, ул. Советская, 14, Ярославль, 150003, Российская Федерация

DOI: 10.18255/1996-5648-2023-3-426-433 Научная статья
УДК 343.2 Полный текст на русском языке

В статье рассматриваются вопросы квалификации кибервымогательства. В частности, данное деяние анализируется как разновидность обычного вымогательства, а также как разновидность исключительно информационного преступления. Делаются выводы, что помимо угроз, характерных для ст. 163 УК РФ, имеют также место и угрозы, которые не входят в перечень способов совершения преступления, перечисленных в указанной статье, а соответственно, и о невозможности привлечения лица к уголовной ответственности за ряд вариаций кибервымогательства по ст. 163 УК РФ. Ввиду того что квалифицировать такие деяния по совокупности ст. 163 и норм УК РФ, посвящённых преступлениям в сфере компьютерной информации, также видится проблематичным, автор считает, что необходимо модернизировать уголовный закон, и предлагает дополнить диспозицию ст. 163 УК РФ новыми способами совершения указанного преступления.

Ключевые слова: компьютерные преступления; кибервымогательство; программы-вымогатели; криптовалюты; уголовный закон

ИНФОРМАЦИЯ ОБ АВТОРАХ

Прудников, Илья Дмитриевич | E-mail: ilya.prudnikov97@gmail.com
Аспирант

Ни для кого не секрет, что с каждым днём информационные технологии всё чаще проникают в нашу жизнь: большинство людей пользуется смартфонами, социальными сетями, а компании постоянно автоматизируют различные рабочие процессы (например, складской учёт, документооборот и прочее). Вместе с тем лица, совершающие преступления, используют подобные технологии для получения доступа к охраняемой законом тайне и информации, торговли наркотиками, оружием и ряда иных незаконных деяний. Одним из вариантов выступает кибервымогательство.

Под кибервымогательством мы понимаем вид обычного вымогательства, при котором выдвигаются определённые в ст. 163 Уголовного кодекса Российской Федерации[1] (далее – УК РФ) имущественные требования 1) за возвращение лицу доступа к компьютерной системе, части компьютерной системы (например, зашифрованным файлам) или информационно-телекоммуникационной сети (обычно браузеру в сети Интернет); 2) некопирование и нераспространение данных, к которым правонарушители получили доступ; 3) отказ от совершения другой кибератаки лицами, совершающими преступление (например, DDoS-атаки).

Для того чтобы проверить, является ли кибервымогательство разновидностью деяния, предусмотренного ст. 163 УК РФ, необходимо сравнить их признаки. У данных правонарушений полностью идентичны признаки субъекта и субъективной стороны, поэтому на них мы позволим себе не останавливаться.

Исходя из местонахождения ст. 163 в УК РФ, основным объектом преступления выступают отношения собственности, а дополнительным – личность, а точнее, здоровье, честь, достоинство, законные интересы [1, с. 376]. Объекты обычного вымогательства, с одной стороны, идентичны объектам кибервымогательства, поскольку при последнем также: а) требуется передать чужое имущество или право на чужое имущество или выполнить иные действия имущественного характера; б) могут дополнительно пострадать здоровье, честь, достоинство, законные интересы личности (например, когда посягающие получают доступ к сведениям, позорящим потерпевшего или его близких, и угрожают такие сведения распространить).

С другой стороны, при одной из самых распространённых вариаций кибервымогательства, когда используются программы-вымогатели (называемые «Ransomware»), дополнительно подвергаются опасности общественные отношения, характерные для преступлений в сфере компьютерной информации. Правонарушители при использовании таких программ, получая доступ к охраняемой законом компьютерной информации, её блокируют, копируют или уничтожают. Сейчас можно назвать два вида подобных программ: программы-блокираторы и программы-шифровальщики. Последний вариант представляет наибольший интерес с точки зрения уголовно-правовой оценки, а также составляет огромную часть деяний, относимых нами к кибервымогательству.

По сведениям компании «Лаборатория Касперского», за период с 2017 по 2020 год от крупнейшего семейства программ-шифровальщиков WannaCry понесли убытки пользователи в 150 странах. Размер этих убытков составил не менее 4 млрд. долларов. Кроме того, некоторые преступные группы, занимающиеся киберпреступлениями, добавляют программы-шифровальщики в свой «арсенал» (например, Lazarus) [2].

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Российская газета. 1996. 18–20 июня (с изм. и доп.).

Об опасности такого рода программ пишут и некоторые исследователи, отмечая, что распространение программ типа «Ransomware» остаётся одной из наиболее значительных угроз в сфере компьютерной информации на протяжении последних лет [3, с. 706].

Атаки, при которых используются программы-шифровальщики, создают ряд проблем:

Первая связана с невозможностью разблокировать данные никаким иным способом, кроме как воспользоваться ключом дешифровки, находящимся у лиц, требующих чужое имущество. Это связано с высокой сложностью используемых алгоритмов шифрования и недостаточной мощностью существующей на настоящий момент в массовом сегменте компьютерной техники. Некоторые авторы отмечают, что подобные программы, используемые правонарушителями и предназначенные для несанкционированной модификации пользовательских данных в компьютерных системах, в большинстве случаев применяют стойкие криптографические алгоритмы, что делает невозможной самостоятельную расшифровку модифицированной информации [3, с. 706];

Вторая проблема связана с высокой сложностью расследования таких деяний, поскольку зачастую пересылаемые атакующим денежные средства направляются в криптовалюте. Криптовалютой признаётся любой вид валюты в цифровой или виртуальной форме. Для защиты транзакций в этой валюте используется шифрование (криптография). Вместе с тем отсутствует центральный орган по выпуску или регулированию криптовалют, а для записи транзакций и выпуска новых единиц используется децентрализованная система [4]. В качестве примера можно назвать Bitcoin или Ethereum. Кроме того, любая из криптовалют может быть обменена на обычные денежные средства.

Итак, предметами преступления, предусмотренного ст. 163 УК РФ, исходя из её диспозиции, выступает чужое имущество; право на имущество; другие действия имущественного характера, совершаемые потерпевшим в пользу вымогающего. Предметом кибервымогательства зачастую являются денежные средства, пересылаемые, как мы отмечали ранее, в криптовалюте.

Возникает вопрос: может ли криптовалюта являться каким-либо из предметов преступления, предусмотренного ст. 163 УК РФ? На наш взгляд, криптовалюта является чужим имуществом. Подобный вывод подтверждается, как минимум:

1) продвижениями в законодательном поле. Например, Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[2] (далее – ФЗ № 259) признаёт цифровую ва-

[2] См.: Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Россий-

люту средством платежа (ч. 3 ст. 1). В силу ч. 3 ст. 14 ФЗ № 259, под организацией обращения в Российской Федерации цифровой валюты понимается деятельность по оказанию услуг, направленных на обеспечение совершения гражданско-правовых сделок и (или) операций, влекущих за собой переход цифровой валюты от одного обладателя к другому, с использованием объектов российской информационной инфраструктуры (то есть прямо написано, что с криптовалютой, как разновидностью цифровой валюты, допустимо совершать, в частности, гражданско-правовые сделки). И хотя ФЗ № 259 устанавливает также некоторые ограничения на оборот такой валюты, например на оплату ею товаров, работ и услуг в определённых обстоятельствах (ч. 5 ст. 14), думается, это не мешает обменивать рассматриваемую валюту на иную (например, на рубли) и обратно;

2) продвижениями в правоприменительном поле. Так, в абз. 3 п. 1 Постановления Пленума Верховного Суда РФ от 07 июля 2015 г. № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем»[3] отмечается, что предметом преступлений, предусмотренных статьями 174 и 174.1 УК РФ, могут выступать в том числе и денежные средства, преобразованные из виртуальных активов (криптовалюты);

3) доктринальными соображениями. Оценивая криптовалюту по четырём признакам предмета преступлений против собственности [5, с. 75], можно отметить, что этот вид ценностей будет подпадать под все признаки, так как он: а) имеет стоимость (*экономический критерий*), ввиду того что данную вариацию валюты можно обменять на привычные денежные средства; б) является результатом деятельности человека (*социальный критерий*), поскольку указанная валюта кем-то выпускается (хотя и не централизованным органом); в) не принадлежит вымогающему лицу на праве собственности (*юридический критерий*), потому что находится в собственности у потерпевшего; г) хотя и не является осязаемым, но по своим свойствам похож, в частности, на безналичные деньги и, следовательно, подпадает под *физический критерий* в рамках исключения.

Объективная сторона вымогательства, исходя из диспозиции ст. 163 УК РФ, заключается, с одной стороны, в имущественных требованиях, а с другой – в угрозах совершить некоторые неблагоприятные для потерпевшего действия. Аналогичные требования и угрозы могут быть осуществлены также в «цифровом мире» и, соответственно, выступать объективной стороной кибервымогательства (например, угрожать насилием или унич-

ской Федерации» // СПС.

[3] См.: Постановление Пленума Верховного Суда РФ от 07 июля 2015 г. № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» // СПС «Консультант Плюс».

тожением чужого имущества правонарушитель может и посредством сообщений в информационно-телекоммуникационной сети Интернет). Так, Т. М. Лопатина справедливо отмечает, что «с точки зрения закона нет разницы, совершено вымогательство в реальной жизни или в виртуальном пространстве» [6, с. 119].

Тем не менее есть одна вариация угроз, которая объективной стороной ст. 163 УК РФ не охватывается. Она относится к воздействию на компьютерную информацию – это блокировка, а равно копирование и распространение указанной информации. Кроме того, в ряде случаев информация может быть уничтожена. Последнее – это единственное, что можно попробовать подвести под диспозицию ст. 163 УК РФ, но в таком случае придётся признать компьютерную информацию имуществом.

Проанализировав компьютерную информацию через призму четырёх ранее названных признаков предмета преступлений против собственности, мы сделали следующие выводы:

1) физическому признаку компьютерная информация отвечает в рамках исключения, поскольку в настоящий момент в качестве предметов имущественных преступлений могут выступать в том числе и нематериальные объекты внешнего мира, например безналичные деньги и бездокументарные ценные бумаги;

2) юридическому признаку указанная информация не соответствует, ввиду того что она должна находиться в собственности у другого лица. В собственности у другого лица может быть лишь имущество, которое является таковым с точки зрения гражданского законодательства. Так, само требование перечислить денежные средства под угрозой уничтожения информации (базы данных) не может быть квалифицировано по ст. 163 УК РФ, несмотря на то что оно направлено на завладение чужим имуществом, так как информация и базы данных не относятся к имуществу с точки зрения гражданского законодательства, а могут лишь в некоторых случаях быть объектом гражданских прав [7, с. 193–194];

3) под экономический критерий рассматриваемая информация подпадает лишь частично, потому что с одной стороны, представляется достаточно трудным оценить стоимость, например, файла курсовой работы; с другой стороны, думается, не очень сложно оценить стоимость подписанного электронной цифровой подписью кредитного договора, где содержатся сведения о должнике и сумма выданных банком денежных средств;

4) социальный признак присутствует, в силу того что компьютерная информация создаётся посредством труда человека.

Исходя из описанного выше, исследуемая информация полностью признакам предмета преступления против собственности не отвечает. Соответственно, признать компьютерную информацию имуществом нельзя.

Таким образом, при кибервымогательстве имеют место угрозы, которые не входят в перечень способов вымогательства, перечисленных в ст. 163

УК РФ. В этой связи, думается, привлечь лицо к уголовной ответственности по ней при угрозе блокирования доступа к данным, их копирования и распространения, а равно уничтожения невозможно.

Кроме того, и признать кибервымогательство сугубо разновидностью преступления, предусмотренного ст. 163 УК РФ, нельзя, потому что имеет место объект (общественные отношения, возникающие в сфере компьютерной информации или обеспечивающие безопасность компьютерной информации [8]), который охраняется нормами гл. 28 УК РФ, а также способы совершения преступления, которые характерны скорее для таких норм, а не для вымогательства. Не является кибервымогательство разновидностью и только преступлений в сфере компьютерной информации, так как оно обладает сильной имущественной составляющей; зачастую правонарушители вымогают у потерпевших имущество, в том числе криптовалюту, которая имеет значительный денежный эквивалент.

Возникает вопрос, можно ли квалифицировать соответствующие действия вымогающих лиц по совокупности ст. 163 и норм УК РФ, посвящённых преступлениям в сфере компьютерной информации. На наш взгляд, нет. Если с квалификацией «компьютерной» составляющей данного деяния проблем не возникает, так как характер реализуемых угроз и действия правонарушителей по использованию программ-вымогателей прямо подпадают под действия ст. 272 и 273 УК РФ (за исключением неправомерного доступа к охраняемой законом компьютерной информации, и ее распространения, поскольку перед распространением информации происходит её копирование), то ст. 163, как отмечалось ранее, не содержит нужного способа совершения преступления.

Исходя из сказанного, можно сделать вывод о необходимости модернизации действующего уголовного закона. Думается, это можно сделать двумя путями: 1) ввести в него новую норму или 2) дополнить ст. 163 УК РФ новыми способами совершения преступления.

Некоторые авторы предлагают пойти по первому пути, обосновывая это, в частности, тем, что включение дополнительного вида угроз непосредственно в диспозицию ч. 1 ст. 163 УК РФ будет перегружать состав, статья будет громоздкой и неудобной в применении [9, с. 143–144]. Мы же считаем, что основания для введения новой нормы отсутствуют.

Угрозы, относящиеся к кибервымогательству не повышают и не понижают общественную опасность и наказуемость деяния по сравнению со способами обычного вымогательства, поскольку между ними нет принципиальной разницы (например, угроза уничтожения имущества очень похожа по уровню общественной опасности на уничтожение компьютерной информации). Кроме того, большинство угроз, свойственных обычному вымогательству, направлены на дополнительный объект. Так, применение насилия направлено на причинение вреда здоровью потерпевшего, а угроза распространения указанных в диспозиции ст. 163 УК РФ сведений –

на причинение вреда чести, достоинству и законным интересам личности. То же самое с угрозами при кибервымогательстве. В соответствии с ранее отмеченным они направлены на воздействие на компьютерную информацию. Следовательно, добавление новых вариаций угроз в виде *блокирования, копирования или уничтожения компьютерной информации либо условия для прекращения блокирования, копирования или уничтожения компьютерной информации* будет органично вписываться в диспозицию ст. 163 УК РФ.

Ссылки

1. Мелентьев А. В. Вымогательство: уголовно-правовая характеристика и современные тенденции // Образование и право. 2020. № 4. С. 375–379.

2. Программы-вымогатели в цифрах: оценка глобального влияния угрозы. URL: https://securelist.ru/ransomware-by-the-numbers-reassessing-the-threats-global-impact/101318/ (дата обращения: 26.04.2023).

3. Россинская Е. Р., Рядовский И. А. Концепция вредоносных программ как способов совершения компьютерных преступлений: классификации и технологии противоправного использования // Всероссийский криминологический журнал. 2020. Т. 14, № 5. С. 699–709.

4. Что такое криптовалюта и как она применяется? URL: https://www.kaspersky.ru/resource-center/definitions/what-is-cryptocurrency.

5. Улезько С. И. Понятие предмета в преступлениях против собственности в современном уголовном праве // Общество и право. 2015. №1 (51). С. 75–78.

6. Лопатина Т. М. Условно-цифровое вымогательство, или кибершантаж // Журнал российского права. 2015. № 1(217). С. 118–126.

7. Грачева Ю. В., Маликов С. В., Чучаев А. И. Предупреждение девиаций в цифровом мире уголовно-правовыми средствами // Право: журнал Высшей школы экономики. 2020. № 1. С. 189–211.

8. Чекунов И. Г. Понятие и отличительные особенности киберпреступности // Российский следователь. 2014. № 18. С. 53-56 // СПС «Консультант Плюс».

9. Овсюков Д. А. Использование информационно-телекоммуникационных сетей при совершении вымогательства // Актуальные проблемы российского права. 2021. № 2 (123). С. 140–145.