УДК 343.7:343.9(045)

С.А. Стяжкина

ВОПРОСЫ КВАЛИФИКАЦИИ КИБЕРВЫМОГАТЕЛЬСТВА

Проблема обеспечения информационной безопасности на сегодняшний день выходит на первые места. Информация становится все более ценным объектом, требующим особой защиты. Общество, трансформируясь в цифровое, все более становится зависимым от информационных ресурсов и информационно-телекоммуникационных сетей. В последнее время широкое распространение получили случаи использования программ-шифровальщиков информации с последующим выдвижением требований уплаты крупных денежных сумм за сохранение данных и их расшифровку. На сегодняшний день отсутствует легальное определение понятия «кибервымогательство». Эти действия подпадают под признаки нескольких преступлений в сфере компьютерной информации, таких как неправомерный доступ к компьютерной информации (ст. 272 УК РФ) и создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ). На наш взгляд, этого недостаточно. При квалификации не учитывается основной объект посягательства – отношения собственности. В связи с чем необходимо скорректировать законодательство в части уголовной ответственности за кибервымогательство. Таким образом, предлагается дополнить ст. 163 УК РФ объективными признаками, направленными на защиту компьютерной информации, либо предусмотреть самостоятельный состав преступления, предусматривающий ответственность за кибервымогательство. Наиболее приемлемым вариантом решения проблемы уголовной ответственности за кибервымогательство является дополнение и расширение ст. 163 УК РФ.

Ключевые слова: кибервымогательство, компьютерная информация, вредоносное программное обеспечение, блокирование информации, вымогательство, неправомерный доступ к компьютерной информации, программы-шифровальщики, требования передачи чужого имущества.

DOI: 10.35634/2412-9593-2022-32-5-941-947

Проблемы обеспечения информационной безопасности на сегодняшний день выходят на первые места. Информация становится все более ценным объектом, требующим особой защиты. Общество, трансформируясь в цифровое, все более становится зависимым от информационных ресурсов и информационно-телекоммуникационных сетей. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденная Указом Президента РФ 9 мая 2017 г. № 203, говорит о том, что «в России информационное общество характеризуется широким распространением и доступностью мобильных устройств, а также беспроводных технологий, сетей связи. Создана система предоставления государственных и муниципальных услуг в электронной форме. Граждане имеют возможность направить в электронной форме индивидуальные и коллективные обращения в государственные органы и органы местного самоуправления. Информационные и коммуникационные технологии оказывают существенное влияние на развитие традиционных отраслей экономики. Информационные и коммуникационные технологии стали частью современных управленческих систем во всех отраслях экономики, сферах государственного управления, обороны страны, безопасности государства и обеспечения правопорядка»[1].

Широкое внедрение цифровых ресурсов во все сферы жизнедеятельности человека, общества и государства требует адекватного правового регулирования вопросов безопасности и защиты информации и информационных ресурсов. Особая роль в сфере обеспечения защиты информации принадлежит уголовно-правовому регулированию охраны информации. Одной из первых сфер, оперативно среагировавших на меняющиеся условия жизни, была криминальная сфера. Информация, представляющая из себя различные сведения, сообщения, данные, может выступать как средством совершения преступления, так и его предметом. Преступники первоначально начали активно использовать информационные ресурсы для совершения преступлений, а затем их интерес стала вызывать и сама информация, которая несет в себе огромный потенциал. Ценность информации заключается не только в ее содержании, но и, с одной стороны, в ее безопасности использования, а с другой - в ее доступности.

[1] Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы, утвержденная Указом Президента РФ 9 мая 2017 г. № 203.

Следует отметить, что на сегодняшний день действующее уголовное законодательство в целом успешно справляется с проблемами уголовно-правового регулирования ответственности за незаконные действия, посягающие на различные виды информации. Достаточно универсальными являются преступления, расположенные в главе 28 УК РФ «Преступления в сфере компьютерной информации». Их количество постоянно увеличивается в общей структуре преступности. Зачастую они выступают способом совершения других преступлений, таких как хищения, незаконное собирание и распространение сведений о частной жизни лица, незаконный оборот наркотиков, вымогательство и многих другие. Часто проблемы возникают при уголовно-правовой оценке действий, которые связаны с посягательством на компьютерную информацию и использованием информационно-телекоммуникационных сетей и их квалификации, которые совершаются в совокупности с другими преступлениями.

В последнее время широкое распространение получили случаи использования программ-шифровальщиков информации с последующим выдвижением требований уплаты крупных денежных сумм за сохранение данных и их расшифровку. Шифровальщики (вымогатели или ransomware) – это разновидность вредоносного программного обеспечения, которое угрожает уничтожить или предотвратить доступ к важным данным жертвы, если она не заплатит злоумышленнику выкуп. К сожалению, этот тип кибератак постоянно набирает обороты: шифровальщики были названы главным типом угроз в 2021 году, ведь только в третьем квартале 2021 года количество атак увеличилось более чем на 140 %[2].

Если в 2020 году киберпреступники, распространяющие программы-вымогатели, угрожали своим жертвам, которые отказывались платить выкуп, передать информацию об атаке их клиентам, то в 2021 году злоумышленники пошли дальше. Теперь они угрожают опубликовать украденные у компании данные, если жертва обратится за помощью в полицию или наймет переговорщика.

В России, по данным компании Group-IB, средняя сумма, которую жертвы переводили киберпреступникам в качестве выкупа, составила 3 млн рублей[3].

В 2021 году чаще всего жертвами программ-шифровальщиков оказывались медицинские и государственные учреждения, научные и образовательные организации, а также промышленные компании. Преступники требуют огромные суммы за разблокировку или расшифровку данных организаций. Естественно, чаще всего объектами посягательств они выбирают крупные компании, обладающие информационными и материальными ресурсами. Но жертвами преступников могут быть и рядовые граждане, активные пользователи Интернета.

Несмотря на широкую распространенность так называемого «кибервымогательства», как в теории, так и в правоприменительной практике нет единства мнений относительно сущности данного явления и его уголовно-правовой оценки. Как пишет Могунова М.Н., «современные научные исследования кибервымогательства ещё не пришли к единому мнению о его юридической природе» [4]. Безусловно, кибервымогательство как относительно новое криминальное явление требует его осмысления с позиций действующего уголовного законодательства, и, возможно, назрела необходимость его дополнительного уголовно-правового регулирования.

Во-первых, необходимо определиться с понятием «кибервымогательство» и его признаками. В литературе существуют различные подходы к рассматриваемому определению. Например, Матросова Л.Д. компьютерное вымогательство относит к разновидностям мошенничества [3]. Лопатина Т.М. рассматривает кибервымогательство как «разновидность информационного преступления, сущность которого заключается в том, что преступник вымогает у потерпевшего денежные средства или иные предметы, имеющие материальную ценность (в том числе криптовалюты), используя угрозы различного характера (как правило, связанные с ограничением доступа к информации пользователя)» [2]. В данной работе не предлагается вводить легальное понятие «кибервымогательство». Представляется, что этот термин будет использоваться для обозначения определенного рода преступных деяний, связанных с неправомерным воздействием на компьютерную информацию (наряду с такими понятиями, как фишинг, скриминг, киберджекинг и т. д.). В рамках рассматриваемого вопроса под «кибервымогательством» предлагается понимать действия лиц, использующих вредоносные компьютерные программы, блокирующие и шифрующие информацию, с последующим выдвижением требований о передаче денежных средств за предоставление доступа к исходной информации и ее дешифровку.

[2] https: // www.securitylab.ru/blog/company/PandaSecurityRus/351920.php
[3] https: // www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021/

Следует отметить, что такие действия подпадают под признаки нескольких статей уголовного кодекса и, как отмечает Гребеньков А.А., «сложности уголовно-правового противодействия кибервымогательству связаны не в последнюю очередь с тем, что оно является комплексным преступлением, сочетающим в себе элементы нескольких составов. Это и составы компьютерных преступлений (прежде всего, создания, использования и распространения вредоносных компьютерных программ и неправомерного доступа к компьютерной информации), и составы преступлений против собственности («классического» вымогательства, если выдвигается угроза распространения каких-либо сведений, которые могут причинить существенный вред правам и законным интересам потерпевшего, а также мошенничества)» [1].

Но проблема квалификации кибервымогательства не только в его комплексности, но и в том, что данные действия не подпадают под признаки вымогательства, которые содержатся в ст. 163 УК РФ, в части выдвигаемых угроз. Преступники, выдвигая требования передачи денежных средств, угрожают уничтожением информации либо ее блокированием. Таких видов угроз ст. 163 УК РФ не предусматривает. Как пишет Мосечкин И.Н., «действующая редакция ст. 163 УК РФ не позволяет охватить все виды угроз, которыми может сопровождаться требование передачи чужого имущества» [5]. И в случае кибервымогательства действия лиц, требующих передачи денежных средств под угрозой блокирования либо уничтожения информации, будут подпадать только под признаки преступлений, предусматривающих ответственность за посягательства на компьютерную информацию. Что касается основной цели преступников – отношения собственности, то она остается без уголовно-правовой оценки. Несмотря на то, что в судебной практике встречаются случаи широкого толкования объектов и видов угроз, являющихся признаками вымогательства (ст. 163 УК РФ), тем не менее квалификация должна проходить строго в соответствии с признаками, изложенными в диспозиции статьи.

В связи с этим Гребеньков А.А. указывает, что кибервымогательство как социально-негативное явление не охватывается ни одним составом преступления, и предлагает включить в уголовное законодательство специальную норму, устанавливающую ответственность за кибервымогательство, под которым предлагается понимать «требование передачи чужого имущества, или права на имущество, или совершения других действий имущественного характера под угрозой уничтожения, повреждения или блокирования компьютерной информации, нарушения функционирования информационных систем» [1]. Во-первых, не совсем ясно, к каким преступлениям будет относится данная норма: к преступлениям против собственности или к преступлениям в сфере компьютерной информации. Во-вторых, вряд ли введение данной нормы решит проблему «комплексности» кибервымогательства.

Такой же позиции придерживается и Овсюков Д.А., предлагая ввести в УК РФ новую статью – 163.1 «Вымогательство в сфере компьютерной информации», в которой следует «предусмотреть ответственность за требование передачи чужого имущества, или права на имущество, или совершения других действий имущественного характера под угрозой совершения компьютерной атаки либо как условие для прекращения атаки» [6].

Прежде всего следует разобраться с признаками рассматриваемого деяния.

Механизм совершения данного преступления состоит из нескольких этапов, и каждый из этапов содержит признаки отдельных преступлений.

Для достижения своих преступных целей, прежде всего, преступнику необходимо внедрить в компьютер вредоносную программу, которая приведет к зашифровке либо блокированию информации потерпевшего. Способов внедрения на сегодняшний день достаточно много. Одним из самых распространенных способов выступает использование электронной почты, на которую приходят файлы, содержащие вирусную программу. Достаточно часто заражение происходит через посещение сайтов, социальные сети и т. д. По данным Positive Technologies, «в атаках на организации основными векторами доставки вредоносного ПО остаются электронная почта (71 %) и компрометация компьютеров, серверов и сетевого оборудования (24 %), а в атаках на частных лиц хакеры отдают предпочтение электронной почте и веб-сайтам (по 32 %)»[4]. Также нередки случаи использования методов социальной инженерии, когда самым слабым звеном в системе защиты информации выступает человек.

Таким образом, речь идет об использовании вредоносной компьютерной программы, ответственность за которое предусмотрена ст. 273 УК РФ. Это выступает способом совершения преступления и требует отдельной квалификации.

[4] https: // www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/

Далее, используя вредоносную компьютерную программу, преступник получает доступ к информации и шифрует или блокирует ее. Кроме того, зачастую преступники, перед тем как зашифровать данные, похищают их. Таким образом, преступники требуют «двойной выкуп»: во-первых, за дешифровку, во-вторых, за неразглашение похищенной информации. Здесь уже речь идет о неправомерном доступе к компьютерной информации, повлекшим ее копирование и блокирование. Данные действия подпадают под признаки ст. 272 УК РФ.

Следующим этапом преступной деятельности выступает требование передачи денежных средств под угрозой ограничения доступа владельцев информации к своим ресурсам, либо уничтожения информации, находящейся на данных ресурсах, либо их распространения. Данные действия, как было отмечено выше, не подпадают под признаки ст. 163 УК РФ, предусматривающей ответственность за вымогательство, так как в статье четко указан перечень угроз. При вымогательстве преступник угрожает применением насилия, либо уничтожением или повреждением чужого имущества, либо распространением сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких. Среди объектов угроз при вымогательстве не указаны информационные ресурсы, компьютерная информация, безопасность информационных технологий и т. д.

Таким образом, на сегодняшний день кибервымогательство подпадает под признаки преступлений в сфере компьютерной информации, таких как неправомерный доступ к компьютерной информации (ст. 272 УК РФ) и создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ). Причем квалификация должна быть с вменением квалифицирующих признаков, предусмотренных в ч. 2 ст. 272 УК РФ и ч. 2 ст. 273 УК РФ - «корыстная цель» и, возможно, «причинение крупного ущерба». Так как лицо, используя компьютерную программу и осуществляя неправомерный доступ к компьютерной информации, преследует цель - извлечение материальной выгоды. Причем следует отметить, что суммы выкупа достаточно большие. Кроме того, очень часто преступники обманывают обладателей информации и разглашают конфиденциальные сведения, причиняя крупный ущерб компаниям. На наш взгляд, такая уголовно-правовая оценка является недостаточной, она не учитывает реальные цели, которые преследую преступники, используя вредоносные компьютерные программы.

Представляется, что все-таки основным объектом посягательства преступников при совершении кибервымогательства выступают отношения собственности. Их основная цель – получение денежных средств. И вред прежде всего причиняется собственности потерпевшего. Информационные ресурсы служат лишь способом получения выгоды материального характера.

В связи с вышеизложенным, необходимо скорректировать законодательство в части уголовной ответственности за кибервымогательство. Как нам представляется, есть несколько вариантов, которые можно предложить для повышения эффективности уголовно-правового противодействия кибервымогательству.

Во-первых, можно пойти по пути, предложенному Гребеньковым А.А., и ввести отдельную статью в Уголовный кодекс, которая бы предусматривала ответственность за кибервымогательство. Например, статью 163.1 УК РФ, которая бы звучала как «требование передачи чужого имущества, права на имущество или совершения действий имущественного характера под угрозой уничтожения, блокирования, модификации, копирования компьютерной информации либо предоставление доступа к ней». В данном определении предусмотрен более широкий перечень угроз, в частности, одной из угроз предлагается ввести угрозу предоставления доступа к компьютерной информации. Речь идет о распространении в сети Интернет корпоративных, конфиденциальных сведений, которые были получены в результате неправомерного доступа к компьютерной информации. Это сведения, ответственность за распространение которых не предусмотрена уголовным законодательством, но распространение которой может причинить вред интересам организаций, компаний, частных лиц.

На наш взгляд, данная норма должна содержаться в главе 21 «Преступления против собственности». И, скорее всего, являться специальной нормой вымогательства, по аналогии с мошенничеством и его видами. Несмотря на вышеизложенное, данное предложение представляется не очень удачным, так как ведет к излишней специализации норм уголовного права, предусматривающих ответственность за вымогательство. Ярким примером неудачной законодательной техники выступает дифференциация ответственности за мошенничество и введение дополнительных многочисленных специальных норм, предусматривающих ответственность за различные виды мошенничества.

Также одним из способов решения возникшей проблемы выступает введение в статью 163 УК РФ дополнительного квалифицирующего признака, предусматривающего ответственность за кибервымогательство. То есть речь идет об ужесточении ответственности за вымогательство, если под угрозу ставится безопасность компьютерной информации. Данный вариант следует установившейся тенденции рассмотрения обстоятельств совершения преступлений в киберпространстве в качестве отягчающего обстоятельства. Хотя такая тенденция и вызывает некие сомнения в обоснованности специализации рассматриваемого признака, тем не менее она получила широкое распространение во многих составах преступлений. Представляется, что совершение преступления с использованием информационно-телекоммуникационных сетей не повышает степени общественной опасности преступления. Проблемы скорее носят организационный характер, а не уголовно-правовой. Сложности раскрытия и изобличения лиц, совершивших данные преступления, зачастую недоступность этих лиц для осуществления правосудия не свидетельствуют о повышенной общественной опасности деяния. Угрозы информационной безопасности по степени общественной опасности не превышают угрозы насилия либо уничтожения или повреждения чужого имущества.

Третьим, наиболее приемлемым вариантом решения проблемы уголовной ответственности за кибервымогательство, является дополнение и расширение ст. 163 УК РФ. О необходимости расширения «перечня вымогательских угроз» не раз указывалось в научной литературе. Не со всеми предложениями можно согласиться, в частности, вызывает сомнения предложение дополнить ст. 163 УК РФ способом «под угрозой совершения иного преступления» [5].

На наш взгляд, следует расширить объекты угроз при вымогательстве, указав в качестве еще одного объекта защиты - безопасность компьютерной информации. Таким образом, предлагается дополнить статью 163 УК РФ положением об угрозах уничтожения, блокирования, модификации, копирования компьютерной информации либо предоставление доступа к ней.

И диспозиция ст. 163 УК РФ с учетом предложенных изменений может звучать следующим образом: «Вымогательство, то есть требование передачи чужого имущества, или права на имущество, или совершения других действий имущественного характера под угрозой применения насилия либо уничтожения или повреждения чужого имущества, а равно под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких, а также под угрозой уничтожения, блокирования, модификации, копирования компьютерной информации либо предоставления доступа к ней».

На наш взгляд, именно дополнение статьи 163 Уголовного кодекса РФ наиболее эффективно и технически грамотно восполнит пробел, существующий на сегодняшний день в уголовном законодательстве в части борьбы с кибервымогательствами, которые набирают все большие обороты.

Таким образом, нет необходимости введения отдельной статьи в Уголовный кодек РФ, которая бы предусматривала ответственность за кибервымогательство. Достаточно расширить существующий состав вымогательства (ст. 163 УК РФ) признаками, относящимися к угрозам причинить вред информационной безопасности субъектов.

Но дополнение статьи 163 УК РФ не решит проблему «комплексности» рассматриваемого преступления. Помимо состава вымогательства, действия преступников необходимо будет квалифицировать по статьям Уголовного кодекса, предусматривающим ответственность за неправомерный доступ к компьютерной информации и за использование вредоносных компьютерных программ, с помощью которых лицо получает доступ к компьютерной информации и шифрует либо блокирует ее.

Подводя итог вышесказанному, следует отметить, что проблемы киберпреступлений, как правило, носят комплексный характер. Как показывает практика, большинство из преступлений в сфере компьютерной информации выступают лишь способом совершения других преступлений, например хищений. Массовое распространение цифровых технологий во всех сферах жизнедеятельности человека привело и к массовой «компьютеризации» преступности. Одной из тенденций развития преступности выступает ее цифровизация. Поэтому неизбежно увеличение количества преступлений, совершаемых в сфере компьютерной информации. Эти преступления чаще всего носят вспомогательный характер и в основной своей массе подлежат квалификации в совокупности с другими преступлениями, ради которых они совершаются. В том числе это касается и преступлений против собственности. На это указывают и разъяснения Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 29.06.2021) «О судебной практике по делам о мошенничестве, присвоении и растрате». В п. 20 ска-

зано, что «Мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по статьям 272, 273 или 274.1 УК РФ». Соответственно, и по другим составам, где преступление совершается посредством неправомерного доступа к компьютерной информации или посредством использования вредоносных компьютерных программ, потребуется дополнительная квалификация по преступлениям в сфере компьютерной информации. Естественно, это будет касаться и кибервымогательства. Нет необходимости создавать новые нормы, ориентируясь только на то, что они совершаются в киберпространстве. Сущность большинства из совершаемых преступлений не меняется, изменяются способы и средства их совершения. А потенциал гл. 28 УК РФ «Преступления в сфере компьютерной информации» позволяет решать возникающие проблемы посредством дополнительной квалификации по составам преступлений, находящихся в этой главе.

В заключение необходимо отметить, что эффективность борьбы с киберпреступлениями зависит не от количества существующих составов, предусматривающих ответственность за их совершение, и не от строгости санкций, а от точности и полноты формулировок норм, предусматривающих уголовную ответственность за рассматриваемые преступления. Количество преступлений в сфере компьютерной информации естественным образом будет увеличиваться, это неизбежный процесс, связанный с информатизацией всех сфер жизни общества и человека. Уголовное законодательство должно своевременно реагировать на изменяющиеся способы и формы преступной деятельности с учетом уже существующих норм и запретов.

СПИСОК ЛИТЕРАТУРЫ

1. Гребеньков А.А. Кибервымогательство как информационное преступление // Экономика, управление и право: инновационное решение проблем: сборник статей IX Международной научно-практической конференции. 2017. С. 154.
2. Лопатина Т.М. Условноцифровое вымогательство, или кибершантаж // Журнал российского права. 2015. № 1. С. 118.
3. Матросова Л.Д. Системный анализ понятия средств реализации и принятия решений по совершенствованию мер защиты от вымогательства в сети Интернет // Закон и право. 2018. № 11. С. 152.
4. Могунова М.М. Уголовно-правовой анализ киберугроз в деловой среде // Вестник Омского университета. Серия «Право». 2021. Т. 18, № 1. С. 86.
5. Мосечкин И.Н. Совершенствование перечня угроз, регламентированного в ст. 163 УК РФ, как мера противодействия вымогательству // Всероссийский криминологический журнал. 2022. Т. 16. № 2. С. 264.
6. Овсюков Д.А. Использование информационно-телекоммуникационных сетей при совершении вымогательства // Актуальные проблемы российского права. 2022. Т. 16 № 2 С. 144.

Поступила в редакцию 05.09.2022

Стяжкина Светлана Александровна, кандидат юридических наук,
доцент кафедры уголовного права и криминологии
ФГБОУ ВО «Удмуртский государственный университет»
426034, Россия, г. Ижевск, ул. Университетская, 1 (корп. 4)
E-mail: styazhkina.sv@yandex.ru

S.A. Styazhkina

QUESTIONS OF QUALIFICATION OF CYBER-EXTORTION

DOI: 10.35634/2412-9593-2022-32-5-941-947

The problem of ensuring information security today comes to the fore. Information is becoming an increasingly valuable object that requires special protection. Society, transforming into a digital one, is becoming increasingly dependent on information resources and information and telecommunication networks. Recently, cases of the use of encryption programs for information have become widespread, with subsequent demands for the payment of large sums of money for the preservation of data and their decryption. To date, "cyber extortion" falls under the signs of crimes in the field of computer information, such as unauthorized access to computer information (Article 272 of the Criminal Code of the Russian Federation) and the creation, use and distribution of malicious computer programs (Article 273 of the Criminal

Code of the Russian Federation). In our opinion, this is not enough. It is proposed to supplement Article 163 of the Criminal Code with additional objective signs aimed at protecting computer information.

Keywords: cyber extortion, computer information, malicious software, blocking of information, extortion, unauthorized access to computer information, encryption programs, demands for the transfer of someone else's property.

Received 05.09.2022

Styazhkina S.A., Candidate of Law, Associate Professor
Udmurt State University
Universitetskaya st., 1/4, Izhevsk, Russia, 426034
E-mail: styazhkina.sv@yandex.ru