DOI: 10.17803/1994-1471.2021.123.2.140-145

Д. А. Овсюков*

Использование информационно-телекоммуникационных сетей при совершении вымогательства

Аннотация. В статье проведен анализ различных видов угроз при совершении преступления, предусмотренного ст. 163 УК РФ, с использованием информационно-телекоммуникационных сетей (ИТС), в том числе Интернета. Выявлены проблемные вопросы при квалификации рассматриваемых деяний, вызванные пробельностью уголовно-правовой охраны отношений собственности при посягательствах с использованием ИТС. Обоснована повышенная общественная опасность угрозы использования информационно-телекоммуникационных сетей, в том числе Интернета, при распространении сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких. Сделан вывод о необходимости дополнения УК РФ новыми нормами, направленными на устранение пробельности уголовно-правовой охраны отношений собственности при посягательствах способом, опасность которого обусловлена быстрым развитием информационных технологий.

Ключевые слова: вымогательство; информационно-телекоммуникационная сеть; Интернет; угроза; компьютерная атака; компьютерная сеть; DDoS; блокирование компьютерной информации; распределенная атака типа «отказ в обслуживании»; компьютерный вирус; преступления против собственности; собственность; преступление; уголовное право.

Для цитирования: *Овсюков Д. А.* Использование информационно-телекоммуникационных сетей при совершении вымогательства // Актуальные проблемы российского права. — 2021. — Т. 16. — № 2. — С. 140–145. — DOI: 10.17803/1994-1471.2021.123.2.140-145.

The Use of Information and Telecommunication Networks in Committing Extortion

Dmitriy A. Ovsyukov, Postgraduate Student, Department of Criminal Law, Kutafin Moscow State Law University (MSAL), Kirov Institute (Branch), Moscow Humanitarian Economic University
ul. Sadovaya-Kudrinskaya, d. 9, Moscow, Russia, 125993
uro-ru@yandex.ru

Abstract. The paper analyzes various types of threats in the commission of a crime under Article 163 of the Criminal Code of the Russian Federation, using information and telecommunication networks (ITS), including the Internet. The problematic issues in classification of the acts under consideration, caused by the lack of criminal law protection of property relations in case of encroachments using ITS, are identified. The increased public danger

© Овсюков Д. А., 2021

* *Овсюков Дмитрий Алексеевич*, соискатель кафедры уголовного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), Кировский институт (филиал) Московского гуманитарно-экономического института
Садовая-Кудринская ул., д. 9, г. Москва, Россия, 125993
uro-ru@yandex.ru

of the threat of using information and telecommunication networks, including the Internet, when disseminating information that dishonors the victim or his relatives, or other information that may cause significant harm to the rights or legitimate interests of the victim or his relatives is substantiated. It is concluded that it is necessary to supplement the Criminal Code of the Russian Federation with new norms aimed at eliminating the gap in the criminal legal protection of property relations in case of encroachments in a way, the danger of which is due to the rapid development of information technologies.

Keywords: extortion; information and telecommunication network; Internet; threat; computer attack; computer network; DDoS; blocking of computer information; distributed denial of service attack; computer virus; property crimes; own; crime; criminal law.

Cite as: Ovsyukov DA. Ispolzovanie informatsionno-telekommunikatsionnykh setey pri sovershenii vymogatelstva [The Use of Information and Telecommunication Networks in Committing Extortion]. *Aktualnye problemy rossiyskogo prava*. 2021;16(2):140-145. DOI: 10.17803/1994-1471.2021.123.2.140-145. (In Russ., abstract in Eng.).

Одним из обязательных признаков объективной стороны вымогательства является угроза, понимаемая как психическое насилие, побуждающее к исполнению предъявленного требования. Обязательные признаки угрозы закреплены в постановлении Пленума Верховного Суда РФ от 17.12.2015 № 56 «О судебной практике по делам о вымогательстве (статья 163 Уголовного кодекса Российской Федерации)». Согласно п. 5 данного документа, угроза должна быть действительной и реальной, т.е. субъективно восприниматься потерпевшим как вполне осуществимая.

Угроза может быть выражена в трех указанных в диспозиции ст. 163 УК РФ формах:

1) угроза применения насилия;
2) угроза уничтожения или повреждения чужого имущества;
3) угроза распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких.

Каждая из этих форм может иметь место с использованием информационно-телекоммуникационной сети (ИТС), в том числе сети «Интернет», путем передачи потерпевшему или иным лицам компьютерной информации, содержащей вышеперечисленные виды угроз.

Угрозой применения насилия следует считать обещание избить, покалечить, убить как лицо, от которого требуют имущество, право на имущество, так и его близких[1]. Близкими лицами могут быть любые лица, значимые для лица, которому адресовано требование. Представляется, что при применении угрозы причинения насилия объектом насилия может быть и иное лицо, не являющееся близким лицом, так как при буквальном толковании ст. 163 УК РФ такого требования не усматривается. Пример такого деяния описан в приговоре Кстовского городского суда Нижегородской области от 14.12.2017. Я. Г. неоднократно обращался к потерпевшему через социальную сеть путем отправки текстовых сообщений с требованием передать денежные средства под угрозой применения насилия[2]. Эти действия судом, как мы считаем, обоснованно были признаны преступлением, предусмотренным ст. 163 УК РФ.

Использовать ИТС для совершения данного вида угрозы можно лишь как средство коммуникации, передачи информации на расстоянии. Остальные способы использования ИТС при совершении преступлений здесь не могут быть применены, так как деяние преступника не направлено на нарушение нормальной работы ИТС или компьютерных систем, входящих в такую сеть.

---

1 Комментарий к Уголовному кодексу Российской Федерации (постатейный) / Г. Н. Борзенков, А. В. Бриллиантов, А. В. Галахова [и др.] ; отв. ред. В. М. Лебедев. 13-е изд., перераб. и доп. М. : Юрайт, 2013.

2 Приговор Кстовского городского суда Нижегородской области от 14.12.2017 по делу № 1-180/2017 // СПС «КонсультантПлюс».

Под угрозой уничтожения или повреждения чужого имущества следует понимать обещание нанести вред имуществу, которое не принадлежит виновному. Как правило, это имущество принадлежит либо адресату требования, либо близким ему лицам. Уничтоженным является имущество, которое полностью утратило свои свойства, функции, не может быть восстановлено и не может использоваться по назначению, либо затраты на восстановление соизмеримы со стоимостью неповрежденного имущества. Поврежденным считается имущество, частично утратившее свои свойства, функции, которое может быть восстановлено и может использоваться по назначению.

В силу того, что предметом преступления является имущество, использование ИТС может быть осуществлено путем коммуникации с лицом, получающим незаконное требование. В то же время при текущем развитии информационных технологий и сетей возможно использование ИТС как средства или способа реализации угрозы. Так, с помощью ИТС можно управлять различными устройствами, подключенными к этой сети. Сейчас эта угроза может распространяться не только на объекты атомной энергетики, механизированные линии на крупных заводах и т.д., вмешательство в которые может повлечь причинение существенного имущественного вреда, но и на бытовые приборы, подключенные к ИТС. Сегодня даже некоторые электрические чайники на кухне могут быть включены через ИТС «Интернет». Несанкционированное включение чайника умозрительно может привести к пожару и существенным имущественным потерям собственника.

При этом следует иметь в виду, что объективной стороной вымогательства охватывается лишь угроза причинения вреда имуществу, а угроза посягательства на компьютерную информацию не может рассматриваться как признак объективной стороны. Это создает проблемы квалификации деяний при блокировании компьютерной информации различными способами и требовании денежного возмещения за разблокирование и продолжение нормального функционирования компьютерной системы. Так, например, при DoS-атаках происходит блокирование сайта или иного сетевого ресурса без его фактического уничтожения[3]. Технология DoS-атаки основана на ограниченности ресурсов атакуемой компьютерной системы. В ходе атаки искусственно организуется масса запросов к системе, с которыми она заведомо не сможет справиться и будет вынуждена отказать в обслуживании. Разновидностью DoS-атаки является DDoS-атака[4], совершаемая одновременно с большого числа компьютеров. Такая атака проводится в том случае, если требуется вызвать отказ в обслуживании более защищенного сайта или сервера.

Суды при квалификации требования передачи денежных средств под угрозой совершения DDos-атаки не выработали единого мнения о квалификации данных деяний как вымогательства. Так, Балаковский городской суд Саратовской области в октябре 2006 г. квалифицировал требование о передаче денежных средств к нескольким компаниям Соединенного Королевства Великобритании и Северной Ирландии за прекращение DDoS-атаки по ст. 163 УК РФ[5]. В 2014 г. Уссурийский районный суд Приморского края действия виновного, который совершил блокирование интернет-сайтов и под угрозой их повреждения выдвигал требование о передаче денежных средств, также квалифицировал по ст. 163 УК РФ[6]. Однако Шпаковский районный суд Ставропольского края требование о передаче денежных средств за прекращение хакерских атак не счел самостоятельно наказуемым деянием и осудил виновного лишь по ст. 272 УК РФ (за организацию DDoS-атаки).

---

[3] DoS-атака (от англ. Denial of Service, отказ в обслуживании) — атака на вычислительную (компьютерную) систему с целью довести ее до отказа, то есть создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам) либо этот доступ будет существенно затруднен.

[4] От анг. Distributed Denial of Service, распределенная атака типа «отказ в обслуживании».

[5] *Сухаренко А. Н.* Транснациональные аспекты российской организованной киберпреступности // Информационное право. 2009. № 3. С. 28–31.

[6] Приговор Уссурийского районного суда Приморского края от 07.05.2014 № 1-458/2014 // СПС «КонсультантПлюс».

Полагаем, что применение ст. 163 УК РФ при совершении угрозы блокирования компьютерной системы будет необоснованно широким толкованием положений УК РФ. Такое толкование хотя и отражает смысл уголовного закона, но не соответствует его букве, так как в деянии не содержится ни одного из видов угроз, перечисленных в ст. 163 УК РФ. Даже если признать компьютерную информацию имуществом, что достаточно спорно, то при DoS- и DDoS-атаках не происходит ее уничтожения или порчи. Она остается в полной сохранности на жестких дисках или иных средствах хранения и лишь временно блокируется. После прекращения атаки либо после отключения атакованной компьютерной системы от сети становится возможно считать информацию без каких-либо проблем.

Еще одним специфическим видом угрозы для совершения мошенничества с использованием информационно-телекоммуникационных сетей является продолжение компьютерной атаки. Такая угроза возникает в том случае, когда блокирование информации предшествует совершению угрозы и не зависит от «сговорчивости» потерпевшего. Угроза же заключается в продолжении блокирования компьютерной информации, сайта или иного сетевого ресурса.

Этот вид угрозы характерен как для DDoS-атак, так и для вирусов-вымогателей, которые вмешиваются в работу компьютерной системы и каким-либо образом мешают ее нормальной работе. За прекращение такого вмешательства виновные требуют перечислить денежные средства на счета, подконтрольные создателям/владельцам вируса. С точки зрения УК РФ компьютерные вирусы признаются вредоносной программой и их создание, распространение или использование квалифицируется по ст. 273.

На текущий момент можно выделить три различных вида вирусов-вымогателей по способу действия:

1) блокировка или помеха работе в системе — вредоносная программа блокирует работу операционной системы и помещает поверх всех окон на рабочем столе сообщение о том, что для восстановления ее работы необходимо перевести денежные средства или их суррогат на определенные счета, электронные кошельки или отправить платное SMS-сообщение. Сообщение на рабочем столе полностью исключает работу либо существенно ее усложняет;
2) блокировка или помеха работе в браузерах — действие вредоносной программы сходно с блокировкой работы операционной системы, только происходит блокировка не всей операционной системы, а лишь интернет-обозревателя;
3) шифрование файлов в системе — действие вируса заключается в обратимой модификации компьютерной информации в целях ее скрытия от законного владельца, пресечения возможности ее использования. Расшифровка компьютерной информации возможна при наличии «ключа», который утверждает выбор конкретного преобразования из совокупности возможных для данного алгоритма шифрования. Для получения «ключа» и разблокирования файлов программа требует перевести денежные средства или их суррогат.

Именно так действует вредоносная программа под названием WannaCry, которая распространилась по всему миру в мае 2017 г. Аналогичным образом функционирует вирус Petya, массовое распространение которого пришлось на июнь 2017 г.

Привлечь к уголовной ответственности за такое требование, выраженное в сообщении вредоносной программы, невозможно, так как в перечне угроз, которые входят в объективную сторону вымогательства, отсутствует как угроза какого-либо воздействия на компьютерную информацию, так и угроза продолжения воздействия на такую информацию.

Делая вывод из вышесказанного, полагаем, что необходимо внести в УК РФ норму о новом виде угроз при совершении вымогательства. Однако включение дополнительного вида угроз непосредственно в диспозицию ч. 1 ст. 163 УК РФ, на наш взгляд, будет перегружать состав, статья будет громоздкой и неудобной в применении, кроме того, не будет охватывать требование о передаче чужого имущества как условие прекращения компьютерной атаки. Поэтому мы считаем необходимым ввести в УК новую статью — 163.1 «Вымогательство в сфере компьютерной информации». В ней следует предусмотреть ответственность за требование передачи чужого имущества или права на имущество или совершения других действий иму-

щественного характера под угрозой совершения компьютерной атаки либо как условия для прекращения атаки. С учетом различной степени общественной опасности угрозы и фактического ее воплощения их следует разместить в различных частях предлагаемой статьи. При этом требование передачи чужого имущества или права на имущество либо совершения других действий имущественного характера как условия прекращения компьютерной атаки будет являться квалифицированным составом.

Квалифицирующие и особо квалифицирующие признаки деяния предлагаем предусмотреть по аналогии со ст. 163 УК РФ: совершение преступления «группой лиц по предварительному сговору», «в крупном размере» — в качестве квалифицирующих признаков; «организованной группой», «в целях получения имущества в особо крупном размере» — в качестве особо квалифицирующих признаков.

Кроме этого, в примечании к предлагаемой статье следует ввести понятие компьютерной атаки следующего содержания: «Под компьютерной атакой понимается совершенное с использованием средств вычислительной техники несанкционированное уничтожение, блокирование, модификация, а также копирование компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей».

Рассмотрев подробно особенности двух первых видов угроз, предусмотренных объективной стороной вымогательства, следует перейти к анализу третьего, и последнего, его вида — угрозы распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких.

В соответствии с упомянутым ранее постановлением Пленума Верховного Суда РФ от 17.12.2015 № 56, под сведениями, позорящими потерпевшего или его близких, понимаются сведения, порочащие их честь, достоинство или подрывающие репутацию, в том числе деловую (например, данные о совершении правонарушения, аморального поступка). К иным сведениям, распространение которых может причинить существенный вред правам или законным интересам потерпевшего либо его близких, следует относить любые сведения, которые составляют охраняемую законом тайну (например, государственная тайна, коммерческая тайна, налоговая тайна, банковская тайна, врачебная тайна, адвокатская тайна, тайна страхования, тайна завещания, тайна усыновления и др.).

Очевидно, что не каждое использование информационно-телекоммуникационной сети является общественно опасным поведением. Так, использование сети для связи между двумя абонентами, которые знают друг друга, является лишь способом коммуникации и не должно свидетельствовать о какой-либо общественной опасности. Как совершенно верно утверждает Е. А. Русскевич, включение квалифицирующего признака в состав преступления необходимо, только если наличие такого признака объективно повышает вероятность наступления вредных последствий[7].

Угроза распространения сведений может как передаваться с помощью информационно-телекоммуникационных сетей, так и реализовываться с их использованием путем размещения порочащей потерпевшего информации на сайтах и иных сетевых ресурсах либо передачи этой информации в личных электронных сообщениях, передаваемых через ИТС. Мы умышленно разделяем эти две формы распространения информации. На наш взгляд, передача позорящих потерпевшего сведений в личных сообщениях мало отличается от традиционной формы распространения сведений путем устного или письменного общения, но размещение информации в публичном доступе имеет более высокую степень общественной опасности.

Так, К. Е. О., имея преступный умысел, направленный на незаконное требование (вымогательство) денежных средств у К., через сеть «Интернет» незаконно потребовал у последней денежные средства в размере 2 500 руб. Реализуя свой преступный умысел, К. Е. О. угрожал распространить в сети «Интернет» фото- и видеоматериалы, которые К. посылала ему только для его личного просмотра[8]. В данной ситуации виновный угрожал распространением порочащих сведений в информационно-теле-

[7] *Русскевич Е. А.* Уголовное право и информатизация // Журнал российского права. 2017. № 8. С. 73–80.

коммуникационной сети «Интернет», к которой имеет доступ индивидуально неопределенный круг лиц.

В другом деле виновный требовал передачи ему денежных средств в сумме 50 000 руб., угрожая распространить сведения, позорящие потерпевшую, передав видеозапись их отношений несовершеннолетнему сыну и родственникам потерпевшей, выложив их в свободный доступ в сети «Интернет»[9].

В рассматриваемых примерах использование ИТС увеличивает степень общественной опасности. Более высокая степень общественной опасности в этом деянии объяснятся тем, что в связи с глобальностью, трансграничностью и распространенностью сети «Интернет» порочащие человека сведения могут быть восприняты в короткий промежуток времени значительным количеством людей, что, безусловно, повышает вероятность наступления вредных последствий и воспринимается потерпевшим как более опасная угроза.

На основании вышеизложенного предлагаем дополнить ч. 2 ст. 163 УК РФ новым квалифицирующим признаком — вымогательством, совершенным с применением угрозы размещения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких, в информационно-телекоммуникационных сетях, включая сеть «Интернет».

По нашему мнению, в случае внесения в УК РФ предложенных изменений будет устранена пробельность уголовно-правовой охраны отношений собственности при посягательствах способом, опасность которого обусловлена быстрым развитием информационных технологий.

БИБЛИОГРАФИЯ

1. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / Г. Н. Борзенков, А. В. Бриллиантов, А. В. Галахова [и др.] ; отв. ред. В. М. Лебедев. — 13-е изд., перераб. и доп. — М. : Юрайт, 2013.
2. *Русскевич Е. А.* Уголовное право и информатизация // Журнал российского права. — 2017. — № 8. — С. 73–80.
3. *Сухаренко А. Н.* Транснациональные аспекты российской организованной киберпреступности // Информационное право. — 2009. — № 3. — С. 28–31.

Материал поступил в редакцию 28 марта 2020 г.

REFERENCES (TRANSLITERATION)

1. Kommentarij k Ugolovnomu kodeksu Rossijskoj Federacii (postatejnyj) / G. N. Borzenkov, A. V. Brilliantov, A. V. Galahova [i dr.] ; otv. red. V. M. Lebedev. — 13-e izd., pererab. i dop. — M. : Yurajt, 2013.
2. Russkevich E. A. Ugolovnoe pravo i informatizaciya // Zhurnal rossijskogo prava. — 2017. — № 8. — S. 73–80.
3. Suharenko A. N. Transnacional'nye aspekty rossijskoj organizovannoj kiberprestupnosti // Informacionnoe pravo. — 2009. — № 3. — S. 28–31.

[8] Приговор Артемовского городского суда Приморского края от 07.11.2016 по делу № 1-470/2016 // СПС «КонсультантПлюс».

[9] Приговор Советского районного суда города Нижнего Новгорода от 07.12.2017 по делу № 1-285/2017 // СПС «КонсультантПлюс».