УДК 343.2/.7

Шебанов Дмитрий Валерьевич

преподаватель кафедры уголовного права и криминологии Воронежского института МВД РФ

Терещенко Любовь Сергеевна

адвокат Воронежской межтерриториальной коллегии адвокатов

О НЕКОТОРЫХ ПРОБЛЕМАХ КВАЛИФИКАЦИИ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Аннотация:
Компьютерная информация в различных ее проявлениях в современном обществе активно используется для обеспечения гражданского оборота и именно поэтому все чаще становится объектом преступных посягательств. В данной статье авторы анализируют недавно включенную в УК РФ норму, предусматривающая уголовную ответственность за мошенничество в сфере компьютерной информации. Ставится под сомнение правильность избранного концептуального подхода законодателя в выделении мошенничества только в определенных сферах общественной деятельности. Представляется не бесспорной актуальность введения уголовно-правовой нормы, предусмотренной ст. 159.6 УК РФ, а также корректность ее содержания; показывается отсутствие логичности в ее конструировании. Отмечаются ее несовершенство и пути его устранения.

Ключевые слова:
уголовное законодательство, компьютерное мошенничество, компьютерная информация, хищение.

Shebanov Dmitry Valeryevich

Lecturer, Criminal Law and Criminology Department, Voronezh Institute of the Ministry of Internal Affairs of Russia

Tereshchenko Lyubov Sergeyevna

Lawyer, Voronezh Interregional Bar Association

CONCERNING SOME PROBLEMS OF FRAUD CLASSIFICATION IN THE COMPUTER INFORMATION FIELD

Summary:
In the contemporary society the computer information in its various manifestations is actively used for civilian traffic, and therefore, is increasingly becoming a target of criminal attacks. The article analyzes the regulation, recently included in the Criminal Code, which envisages criminal liability for fraud in the field of computer information. The authors dispute the correctness of the chosen conceptual approach of the legislator to consider the fraud only in some certain areas of the public activity. The introduction of the criminal legal regulation, specified in the article 159.6 of the Criminal Code of the Russian Federation, seems to be questionable, as well as the correctness of its content. The authors show the lack of consistency in the article 159.6 of the Criminal Code, state its weak points and ways to improve them.

Keywords:
criminal law, computer fraud, computer information, theft.

Технический прогресс, безусловно, является в большей степени позитивным явлением, улучшающим условия существования людей, делающим эту жизнь более комфортной. Однако, к нашему величайшему сожалению, технический прогресс имеет и обратную сторону, неся ряд негативных последствий. Одно из них – развитие новых направлений преступной деятельности, связанной с применением новейших технологий.

Одним из таких преступных деяний, потребовавших внесения изменений в действующее уголовное законодательство, стало мошенничество в сфере компьютерной информации. Случаи мошенничества, в основе которых лежит использование разнообразной экономически значимой компьютерной информации, в настоящее время получают все большее распространение. Многие пользователи компьютерной информации не уделяют должного внимания ее защите, тем самым облегчая действия мошенников.

Введение ст. 159.6 в УК РФ свидетельствует о том, что законодатель пошел по пути выделения из общего частного, к криминализации отдельных разновидностей мошенничества, в данном случае в сфере компьютерной информации и средств хранения, обработки или передачи ее или информационно-телекоммуникационных сетей. Очевидно, что законодательные новеллы связаны со стремлением государства усилить борьбу с новыми преступными проявлениями, характерными для общества с рыночной моделью жизнедеятельности [1].

Следует отметить, что введенные ранее в УК РФ специальные виды мошенничества [2] охватывались общей нормой ст. 159 УК РФ «Мошенничество». В этой связи ряд авторов [3] совершенно справедливо подвергают сомнению необходимость дополнительного выделения и криминализации отдельных видов мошеннических деяний в российском уголовном законе [4].

Кроме того, новая норма уголовного кодекса, а именно ст. 159.6, порождает немало споров из-за несовершенства своей конструкции, что спровоцировало большое разнообразие научных подходов, среди которых автор выделил бы две основных концепции криминализации компьютерного мошенничества.

Имплементарный подход выражается в унификации уголовного законодательства с общеевропейскими нормами в рамках Конвенции Совета Европы «О киберпреступности» (Council of Europe Conventionon Cyber-crime), где данное преступление сформулировано наиболее широко: в качестве любого вреда имущественного характера, причиненного неправомерной манипуляцией с компьютерной информацией [5]. Подобный же подход реализован в законодательстве США, предусматривающем четыре состава мошенничества с использованием компьютерных технологий [6]. Следуя указанному подходу, понятие компьютерного мошенничества включает признаки, содержащиеся в различных статьях отечественного УК РФ. При этом само компьютерное мошенничество является обманом для данной системы, а не человека, и поэтому должно квалифицироваться как кража. На практике же данный принцип соблюдается с точностью до наоборот. Подобное положение дел может быть объяснено тем, что само понятие «компьютерное мошенничество» сложилось стихийно-исторически под воздействием представителей не только юридической науки, но и специалистов по информационной безопасности, заимствовавших свои представления у западных коллег [7].

Представляется, что данный подход имеет существенные недостатки, нарушающие логику построения отечественного уголовного закона.

Более логичным автору видится традиционно-расширительный подход, основанный на гармонизации формы и содержания международных уголовно-правовых норм в процессе интеграции их в отечественное уголовное законодательство. Т.Л. Тропина предлагает криминализировать компьютерное мошенничество, используя понятие хищения в ст. 159.1 УК РФ: «Хищение чужого имущества или приобретение права на чужое имущество, совершенное путем ввода, изменения, удаления или блокирования компьютерных данных либо другого вмешательства в функционирование компьютера или компьютерной системы» [8], тем самым исключая противоречия в понимании компьютерного мошенничества, присущие имплементарному подходу.

Следует отметить, что из введенных в УК РФ ст. 159.1–159.6, «Мошенничество в сфере компьютерной информации» является единственной нормой, существенно отличающейся от традиционной ст. 159. Ведь если вышеназванная статья дает определение мошенничества и диспозиции введенных в кодекс Федеральным законом от 29 ноября 2012 г. № 207-ФЗ ст. 159.1–159.5 в той или иной мере соответствуют этому определению, то объективная сторона «компьютерного мошенничества» существенно разнится с данным понятием, так как содержит абсолютно иной способ совершения хищения. Напомним, согласно диспозиции ст. 159, обязательный признак мошенничества – это способ «путем обмана или злоупотребления доверием». В норме, предусмотренной ст. 159.6, указанный признак отсутствует и появляется абсолютно новый способ совершения хищения: «…путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей». Как видим, ни о каком обмане либо злоупотреблении доверием в диспозиции рассматриваемой статьи речи не идет. Это логично, поскольку обмануть машину, то есть бездушную вещь, лишенную психики, невозможно. Чем, прежде всего, отличалось традиционное мошенничество – прямым или виртуальным, но обязательно контактом с живым лицом. В предложенной законодателем норме это становится неактуальным. Гораздо большее сходство данная статья имеет с нормами, предусмотренными гл. 28 УК РФ. Однако, не случайно (как хочется верить) законодатель поместил ее в другую главу, подчеркнув тем самым важность такого объекта посягательства как собственность. Рассматривая в данном контексте ст. 159.6 можно сделать довольно необычный, но логичный вывод – любое хищение (кража, мошенничество, присвоение или растрата), совершенное вышеуказанным способом, подпадает под действие этой уголовно-правовой нормы. Если это не так и мы будем придерживаться традиционного определения мошенничества, то смысла в введении ст. 159.6 как отдельной нормы УК РФ абсолютно нет, так как и следственная и судебная практика показывает, что мошенничества, совершенные с использованием компьютерных технологий, довольно успешно расследовались и рассматривались в судах и по ст. 159 УК РФ. Если же мы все-таки примем новый подход, то невооруженным глазом видна необходимость исключения из названия и диспозиции части первой термина «мошенничество». В противном случае возможна громадная неразбериха в деятельности органов предварительного следствия и суда. С одной стороны, определение – мошенничество (дано в ст. 159 УК РФ), с другой – новый способ совершения хищения.

Вчитайтесь внимательно и вдумайтесь в диспозицию ст. 159.6, и вы поймете, о чем идет речь.

Раскрывая все понятия, дословно там написано следующее: хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием в сфере компьютерной информации, то есть хищение чужого имущества или приобретения права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Говоря современным языком – два в одном, то есть в одной диспозиции два разных определения способа совершения преступного деяния. Конечно, на это можно взглянуть и с другой стороны, представив, что законодатель дал нам новое определение мошенничества. Но и тогда получается довольно необычная картина. В одной главе уголовного закона два разных определения преступления, называемого мошенничеством. Поэтому мы все-таки предлагаем изменить терминологию в рассматриваемой статье, назвав ее просто «Хищения в сфере компьютерной информации». На наш взгляд это не только устранит неразбериху в определении мошенничества, но и поспособствует гораздо лучшему раскрытию и уж тем более расследованию преступлений в данной сфере, так намного упрощается процесс квалификации.

Вернемся к тому, что мошенничество подразумевает обязательный (прямой или виртуальный) контакт преступника с жертвой. Как тогда быть в случае, если в результате тайного вмешательства в чью-либо компьютерную информацию, опять-таки очень тайно совершается хищение имущества (неважно – деньги с расчетного счета, активы, имеющие соответствующий денежный эквивалент и т.п.)? Согласно традиционному подходу, это кража. Как квалифицировать действия лица, который совершает хищение указанного выше имущества с помощью компьютерной информации, но если оно было ему вверено? Традиционно – это присвоение или растрата. Для чего тогда вводилась статья, где в диспозиции прямо указывается «…хищение чужого имущества или приобретения права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей»? На наш взгляд, именно для облегчения квалификации, расследования и судебного разбирательства именно различных форм хищений, совершенных в сфере компьютерной информации. Однако, предлагая название «Хищения в сфере компьютерной информации», мы упускаем из вида один немаловажный момент. Как быть, если с помощью и в сфере компьютерной информации, например, путем ее блокирования, с целью получения имущественной выгоды, происходит банальный шантаж. Легального определения шантажа в нашем уголовном законодательстве нет, о чем мы уже говорили в своей статье «О некоторых аспектах определения вымогательства» [9]. Вышеуказанные преступные действия можно было бы квалифицировать по ч. 2 ст. 272 УК РФ, если бы не одно большое «но» – объект. Преступник, прежде всего, посягает на собственность с помощью блокирования компьютерной информации, шантажируя этим самым жертву, но все-таки именно собственность потерпевшего выступает в данном случае в качестве основного объекта посягательства. Выход из сложившейся ситуации в принципе есть. Если принять на законодательном уровне то определение хищения, которое предлагалось нами в статье «Некоторые проблемы квалификации хищений» [10], и иное определение вымогательства: «как вымогательство в статьях настоящего кодекса следует понимать совершенное с корыстной целью или из иной личной заинтересованности понуждение лица к соответствующему волеизъявлению в пользу виновного или третьих лиц» [11], то вымогательство, практически без проблем можно будет назвать одной из форм хищения и рассматриваемое нами деяние полностью подпадает под действие ст. 159.6 УК РФ с названием «Хищения в сфере компьютерной информации».

Ссылки:

1. Шеслер А. Мошенничество: проблемы реализации законодательных новелл // Уголовное право. 2013. № 2. С. 67–71.
2. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 03.02.2014 г.) // Собр. законодательства РФ. 17.06.1996 г. № 25. Ст. 2954.
3. Комаров А.А. Об уточнении понятия «компьютерное мошенничество» в свете законодательных инициатив Верховного Суда РФ // Юрист. 2013. № 17. С. 33–36.
4. Федеральный закон от 29.11.2012 г. № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» // Собр. законодательства РФ. 03.12.2012 г. № 49. Ст. 6752.
5. Комаров А.А. Указ. соч.
6. Волеводз А.Г., Волеводз Д.А. Уголовное законодательство об ответственности за компьютерные преступления: опыт разных стран // Правовые вопросы связи. 2004. № 1. С. 37–48.
7. Комаров А.А. Указ. соч.
8. Тропина Т.Л. Киберпреступность: Понятие, состояние, уголовно-правовые меры борьбы: автореф. дис. … канд. юрид. наук. Владивосток, 2005. С. 13.
9. Терещенко Л.С., Шебанов Д.В. О некоторых спорных аспектах определения вымогательства // Бизнес в законе. 2013. № 6. С. 85–89.
10. Терещенко Л.С., Шебанов Д.В. Некоторые проблемы квалификации хищений // Пробелы в российском законодательстве. 2013. № 6. С. 163–167.
11. Терещенко Л.С., Шебанов Д.В. О некоторых спорных аспектах …

References:

1. Shesler, A 2013, 'Fraud: Implementation Challenges legislative developments', *Criminal Law,* no. 2, p. 67-71.
2. 'Criminal Code of the Russian Federation of 13.06.1996, № 63-FZ (as amended on 03.02.2014)' 1996, *Coll. of legislation of the Russian Federation*, 17.06, no. 25, art. 2954.
3. Komarov, AA 2013, 'For clarification of the concept of "computer fraud" in light of the legislative initiatives of the Supreme Court', *Lawyer,* no. 17, p. 33-36.
4. 'Federal Law of 29.11.2012, № 207-FZ "On Amendments to the Criminal Code of the Russian Federation and Certain Legislative Acts of the Russian Federation"' 2012, *Coll. of legislation of the Russian Federation,* 03.12, no. 49, art. 6752.
5. Komarov, AA 2013, 'For clarification of the concept of "computer fraud" in light of the legislative initiatives of the Supreme Court', *Lawyer,* no. 17, p. 33-36.
6. Volevodz, AG & Volevodz, DA 2004, 'Criminal law on liability for computer crime: the experience of different countries', *Legal issues of communication,* no. 1, p. 37-48.
7. Komarov, AA 2013, 'For clarification of the concept of "computer fraud" in light of the legislative initiatives of the Supreme Court', *Lawyer,* no. 17, p. 33-36.
8. Tropina, TL 2005, *Cybercrime: The concept, the state penal measures against,* PhD thesis abstract, Vladivostok, p. 13.
9. Tereshchenko, LS & Shebanov, DV 2013a, 'Some controversial aspects of the definition of extortion', *Business in law,* no. 6, p. 85-89.
10. Tereshchenko, LS & Shebanov, DV 2013b, 'Some problems of qualification theft', *Gaps in Russian legislation,* no. 6, p. 163-167.
11. Tereshchenko, LS & Shebanov, DV 2013a, 'Some controversial aspects of the definition of extortion', *Business in law,* no. 6, p. 85-89.