Научный журнал «Эпомен», № 75, 2023 | Epomen Scientific Journal, No. 75 (2023)
DOI: 10.58589/26866722_2023_75_105
УДК/UDC 343.721

Компаративистский анализ зарубежного законодательства стран англосаксонской правовой семьи и норм российского уголовного законодательства об ответственности за мошенничества с использованием информационно-телекоммуникационных технологий

Петрякова Людмила Александровна
преподаватель кафедры уголовного права юридического института
Иркутский государственный университет
г. Иркутск, Россия
e-mail: poimanowa@mail.ru
SPIN-код: 3607-4003

Асташкина Полина Дмитриевна
студентка юридического института
Иркутского государственного университета
Иркутск, Россия
e-mail: p.astashkina52@gmail.com

Аннотация

В статье проанализировано уголовное законодательство некоторых зарубежных стран англосаксонской правовой семьи и нормы российского уголовного законодательства относительно вопросов квалификации таких составов преступлений как мошенничество с использованием информационно-телекоммуникационных технологий. Установлено, что в Уголовном кодексе РФ ответственность за мошенничество с использованием информационно-телекоммуникационных технологий наступает по ст. ст. 159, 159.3 и 159.6 УК РФ. Проведенное исследование позволило установить несколько подходов уголовно-правовой квалификации мошенничеств с таким способом по законодательству некоторых стран англосаксонской правовой семьи: как самостоятельный специальный состав преступления; как квалифицирующий признак; отсутствие самостоятельного состава, но указание на признак использования информационно-телекоммуникационных технологий в общем составе и др. Установлено, что в некоторых государствах кибермошенничества рассматривается не как преступления против собственности, а как преступления в сфере компьютерных технологий, что является отличительной особенностью в отношении подхода Российской Федерации при определении объекта данного вида преступных деяний.

Ключевые слова: мошенничество, мошенничество с использованием информационно-телекоммуникационных технологий, киберпреступность, сравнительный анализ, зарубежное законодательство.

Comparative analysis of foreign legislation of the countries of the Anglo-Saxon legal family and the norms of Russian criminal law on liability for fraud using information and telecommunication technologies

Petryakova Lyudmila Alexandrovna
Lecturer of the Department of Criminal Law
Law Institute
Irkutsk State University
Irkutsk, Russia
e-mail: poimanowa@mail.ru
SPIN code: 3607-4003

Astashkina Polina Dmitrievna
Student of the Institute of law
Irkutsk State University
Irkutsk, Russia
e-mail: p.astashkina52@gmail.com

Abstract

The article analyzes the criminal legislation of some foreign countries of the Anglo-Saxon legal family and the norms of Russian criminal legislation regarding the qualification of such crimes as fraud using information and telecommunication technologies. It is established that in the Criminal Code of the Russian Federation, responsibility for fraud using information and telecommunication technologies comes under Articles 159, 159.3 and 159.6 of the Criminal Code of the Russian Federation. The conducted research allowed us to establish several approaches to the criminal legal qualification of fraud in this way under the legislation of some countries of the Anglo-Saxon legal family: as an independent special corpus delicti; as a qualifying feature; the absence of an independent composition, but an indication of the use of information and telecommunication technologies in the general composition, etc. It has been established that in some states cyberbullying is considered not as crimes against property, but as crimes in the field of computer technology, which is a distinctive feature in relation to the approach of the Russian Federation in determining the object of this type of criminal acts.

Key words: fraud, fraud using information and telecommunication technologies, cybercrime, comparative analysis, foreign legislation.

На сегодняшний день развитие глобальной компьютерной сети интернет и информационно-телекоммуникационных технологий является неоспоримым преимуществом, которым обладает нынешнее поколение. Однако, несмотря на все возможные блага, такие как: улучшение коммуникаций; возможность работать и учиться дистанционно;

увеличение продукции из сферы развлечений и др., существует и иная сторона, это упрощение совершения разного рода преступлений.

Использование информационно-телекоммуникационных технологий возможно в различных преступных посягательствах (в частности, в данную группу входят кража, мошенничество, присвоение или растрата, совершенные с использованием компьютерных технологий, незаконный оборот компьютерных программ, предназначенных для осуществления транзакций, манипулирование рынком, хищение радиоактивных материалов, наркотических средств, психотропных веществ, их аналогов и прекурсоров, незаконный интернет-оборот порнографических материалов, незаконное получение государственных, коммерческих и банковских секретов посредством применения информационных технологий и проч.) [1]. Несомненно, количество преступлений, в которых преступники прибегают к способам совершения деяний осложненных технической стороной велико, однако, в рамках настоящего исследования, внимание было уделено мошенничеству с использованием информационно-телекоммуникационных технологий. Каждое государство устанавливает собственную систему регулирования и установления признаков, определяющих в дальнейшем возможность отнесения деяния в ту или иную группу преступлений исходя из нескольких оснований:

– принадлежность страны к определенной правовой семье (англосаксонская правовая семья; романо-германская правовая семья; страны СНГ и страны азиатского региона);

– определение подхода к квалификации рассматриваемого преступления (выделение преступления в самостоятельный специальный состав; определение признака «с использованием информационно-телекоммуникационных технологий» как квалифицирующий; отсутствие специального состава как такового и др.).

В связи с выявленными особенностями было приято решение в проведении компаративистского анализа уголовно-правовых норм России и стран англосаксонской правовой семьи по вопросу квалификации мошенничества с использованием информационно-телекоммуникационных технологий.

Проведение такого рода исследования позволит определить наличие или отсутствие возможности интегрировать сложившиеся в практике зарубежных стран подходы к квалификации обозначенного выше преступления.

Ученые отмечают особую роль сравнительных исследований в рамках противодействия глобальным проблемам современности, т.к. для достижения положительного результата государствам необходимо принять единообразную политику предотвращения наступления неблагоприятных последствий, что возможно только путем внедрения единообразной системы норм права, которая должна эффективно выполнять свою функцию в условиях любой национальной правовой системы [2].

Так, в странах англосаксонской правовой семьи особое внимание уделяется судебному прецеденту, который в данной правовой семье выступает одним из источников права, что не свойственно другим правовым семьям. Однако, принадлежность к одной правовой семье вовсе не означает, что нормы о мошенничестве с использованием информационно-телекоммуникационных технологий обязательно будут совпадать.

При анализе уголовного законодательства таких стран как США, Великобритания, Канада и Новая Зеландия была выявлена общая тенденция при квалификации мошенничества с использованием информационно-телекоммуникационных технологий или преступлений обманного характера, как наличие самостоятельной специальной

уголовно-правовой нормы, устанавливающей ответственность за такой вид преступного деяния.

Согласно Своду законов США, составы мошенничества относятся к главе 47 «Мошенничество и ложные заявления». Сама глава объединяет в себе достаточно большое количество составов и непосредственно видов мошенничества, однако в рамках проводимого исследования особый интерес представил §1030 «Мошенничество и сопряженная с ним деятельность, связанная с компьютерами». Согласно данному параграфу: тот, кто сознательно и с намерением обмануть получает доступ к защищенному компьютеру без авторизации или превышает разрешенный доступ, и посредством такого поведения способствует предполагаемому мошенничеству и получает что-либо ценное, если только объект мошенничества и полученная вещь не состоят только из использования компьютера и ценности такого использование составляет не более 5000 долларов США в течение любого годичного периода [3]. Стоит отметить, что, несмотря на первоначальное сходство, данная норма толкуется иначе, чем предусмотренная УК РФ нома об ответственности за мошенничество в сфере компьютерной информации (ст. 159^6 УК РФ). Ч. 1 ст. 159^6 УК РФ определяет, что хищение чужого имущества или приобретение права на чужое имущество осуществляется посредством использования компьютерной информации путем ввода, удаления, блокирования, модификации и иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей [4], т.е. конструктивным признаком такого преступного деяния является использование компьютерной информации, и законодателем установлен открытый перечень действий, посредством которых возможно осуществить использование.

Норма Свода законов США содержит два необходимых действия, первое – получение доступа к защищенному компьютеру без авторизации, либо превышение разрешенного доступа, вторым же действием будет являться непосредственно совершение мошенничества. С нашей точки зрения, отсутствием в норме указания на конкретные действия, совершаемые при использовании компьютера, законодатель лишь обозначает, что мошенничество совершается посредством использования компьютера, однако каким образом будет использовано указанное средство преступления значения для квалификации не имеет. Важным признаком является намерение преступника использовать компьютер именно с целью совершения дальнейшего мошенничества.

Еще одной особенностью мошенничества и сопряженной с ним деятельностью, связанной с компьютерами, является указание законодателя на возможный продолжаемый характер деяния (продолжаемое преступление), так как, имущественный ущерб в результате обманного хищения с использованием компьютера может быть причинен в результате нескольких тождественных действий, совершенных за один календарный год, и сумма общего ущерба, нанесенного преступником за обозначенный период не должна быть менее 5000 долларов США.

В уголовном законодательстве Великобритании содержится схожая по содержанию норма со ст. 159^{6} УК РФ, устанавливающая уголовную ответственность за совершение мошенничества с использованием компьютерных технологий. Однако, в Законе о преступлениях обманного характера 2006 г. предусмотрены нормы, аналогов которым в уголовном законодательстве иных зарубежных стран нет. Разделы 6 и 7 Закона о преступлениях обманного характера 2006 г. предусматривают уголовную ответственность за владение, изготовление и поставку предметов, используемых для мошенничества.

Содержание раздела 6 Закона о преступлениях обманного характера 2006 г. выражается во владении или осуществлении контроля над любым предметом (включая любую программу или данные в электронной форме), предназначенным для использования в преступлениях обманного характера [5]. Стоит отметить, что норма не подразумевает выполнение объективной стороны мошенничества при данном составе преступления, однако наличие ответственности за подобного рода деяния отражает намерение законодателя привлекать к ответственности за действия подготовительного характера к совершению мошенничества. Считать данные разделы затрагивающими мошенничество с использованием информационно-телекоммуникационных технологий позволяет указание на предмет, которым владеет, изготавливает либо поставляет преступник. Это могут быть как специальные программы, при помощи которых осуществляются мошеннические схемы: QFM – мошенничество с программами ввода-вывода данных; QFP – мошенничество с платежными средствами посредством использования компьютера, а также иного технического оборудования и др.; так и данные в электронной форме, что в конечном итоге указывает не только на использование, но и в отдельных случаях на создание оборудования относимого к информационно-телекоммуникационным технологиям.

Стоит так же отметить, что данный состав преступления по конструкции объективной стороны является формальным. Для наступления уголовной ответственности отсутствует необходимость в возникновении каких-либо последствий или имущественного ущерба, нанесенного собственнику. Так же для квалификации по данному составу преступления нет надобности в совершении последующего мошенничества. Достаточно лишь владеть либо изготовить предмет целью использования которого является мошенническое действие.

В уголовном кодексе Канады ст. 403 установлена уголовная ответственность за мошенничество с использованием личных (идентификационных) данных потерпевшего. Для того, чтобы понять, что канадский законодатель имеет в виду под понятием личные (идентификационные) данные, следует обратиться к ст. 402.1 УК Канады. Кроме очевидных имени, адреса, даты рождения и др. данных сюда же относятся «…электронная подпись, цифровая подпись, имя пользователя, кредитный номер карты, номер дебетовой карты, пароль…» [6]. Тем самым, проведя аналогию с российским уголовным правом можно сделать вывод, что данная норма содержит в себе два отдельных состава предусмотренных УК РФ, а именно ст. 159^3 УК РФ (Мошенничество с использованием электронных средств платежа), за тем исключением, что в канадской норме предусмотрено лишь использование данных электронного средства платежа и не подразумевается использование физического средства платежа (кредитные и дебетовые карты); ст. 159^6 УК РФ (Мошенничество в сфере компьютерной информации), поскольку под личными (идентификационными) данными в УК Канады понимаются электронная и цифровая подпись, имя пользователя, пароли и иные данные, относящиеся к компьютерной информации. Но канадский уголовный закон, в отличие от российского, не выделяет способы использования указанных данных, что позволяет сделать вывод, что любое использование таких данных с целью мошенничества подпадает под действие ст. 403 УК Канады.

В уголовном кодексе Новой Зеландии также имеются нормы о мошенничествах с использованием информационно-телекоммуникационных технологий, однако интересным является то, что отнесено данное преступление не к преступлениям против собственности, а к главе о преступлениях, связанным с компьютерами.

Ст. 249 УК Новой Зеландии предусматривает уголовную ответственность за доступ к компьютерной системе с нечестной целью. Доступ к компьютерной системе с нечестной целью законодателем раскрывается как прямое или косвенное получение доступа к любой компьютерной системе и таким образом, нечестное или путем обмана, без предъявления прав получение любой собственности, привилегии, услуги, денежного преимущества, выгоды и ценного вознаграждения [7]. И отнесение такого состава преступления именно к компьютерным преступлениям является логичным и обоснованным.

С той формулировкой деяния, которую предлагает новозеландский законодатель, на первый план выходит не хищение чужого имущества посредством обмана, а действия, осуществляемые с компьютером, т.е. сам доступ к компьютерной системе, использование которой имеет цель на дальнейшее совершение мошенничества. Однако, остается неясным, следует ли в данном случае последствие в виде уголовной ответственности только по данной норме уголовного закона или мошенничество с доступом к компьютерной системе, а соответственно мошенничество с использованием такой системы являет собой совокупность общего состава о мошенничестве и дополнительно вменяется доступ к компьютерной системе с нечестной целью. Стоит отметить, что норма разделена на оконченное и неоконченное преступление. Моментом окончания данного преступления выступает получение преступником имущественной выгоды в виде завладения чужим имуществом с использованием компьютерной системы.

Подводя итоги проведенного исследования было установлено, что несмотря на принадлежность стран к одной правовой семье, каждое государство по-разному подходит к решению вопроса не только о квалификации, но и о криминализации того или иного деяния охватывающего мошенничество с использованием информационно-

телекоммуникационных технологий. Нормы являются нетождественными по содержанию общественных отношений, которым причиняется вред в результате совершения кибермошенничества. Как было установлено, такого рода преступления могут рассматриваться не только в рамках составов о преступлениях против собственности, но и быть охвачены разделами и главами, посвященными преступлениям против компьютерной безопасности.

В абсолютном большинстве исследуемых стран, так или иначе установлены нормы, позволяющие квалифицировать деяние не по общему составу мошенничества, а прибегнуть к специальным составам. Однако, при анализе уголовного законодательства стран англосаксонской правовой семьи не было выявлено специальной единой нормы, по которой было бы возможно квалифицировать мошенничество с использованием информационно-телекоммуникационных технологий. Ближе всего к такой формулировке нормы подошел Свод законов США, устанавливающий ответственность за мошенничество, посредством использования компьютерной техники. Стоит отметить, что на сегодняшний день и в российском законодательстве отсутствует специальная норма для квалификации таких деяний, в связи с чем в зависимости от обстоятельств, квалификация осуществляется по трем нормам – ст. ст. 159, 159^3 и 159^6 УК РФ.

По нашему мнению, базируясь на опыте квалификации кибермошенничеств стран англосаксонской правовой семьи и учитывая особенности системы российского национального права, нет необходимости в создании самостоятельной нормы посвященной мошенничеству с использованием информационно-телекоммуникационных технологий в уголовном законодательстве Российской Федерации. На сегодняшний день более удачным вариантом представляется разработка квалифицирующего признака "мошенничество

с использованием информационно-телекоммуникационных технологий" в ст. 159 УК РФ, так как нельзя отрицать, что мошенничество с указанным способом совершения преступления представляет более повышенную общественную опасность в отношении ч. 1 ст. 159 УК РФ.

Список литературы:

1. Семыкина О. И. Противодействие киберпреступности за рубежом // Журнал зарубежного законодательства и сравнительного правоведения. 2016. № 6(61). С. 104-113.
2. Зернов А. О., Воскресенская Е. В., Индык К. П. Сравнительные исследования: разновидности и роль в правовых науках // The Scientific Heritage. 2021. № 70-4(70). С. 33-35.
3. U. S. Code // Legal Information Institute. URL: https://www.law.cornell.edu/uscode/text/18/1030 (дата обращения 18.11.2022).
4. Уголовный кодекс Российской Федерации: федеральный закон от 13.06.1996. № 63-ФЗ // Собрание Законодательства Российской Федерации. 1996. № 25. Ст. 2954.
5. Fraud Act 2006 // The Crown Prosecution Service. URL: https://www.cps.gov.uk/legal-guidance/fraud-act-2006 (дата обращения 19.11.2022).
6. Criminal Code // Justice Laws Website. URL: https://laws-lois.justice.gc.ca/eng/acts/c-46/page-54.html#h-122702 (дата обращения 20.11.2022).
7. Crimes Act 1961 // New Zealand Legislation. URL: https://legislation.govt.nz/act/public/1961/0043/latest/DLM330422.html (дата обращения 20.11.2022).

References:

1. Quote from: Semykina, O. I. Countering cybercrime abroad // Journal of Foreign Legislation and Comparative Jurisprudence. 2016. No. 6(61). pp. 104-113.
2. Zernov, A. O., Voskresenskaya E. V., Indyk K. P. Comparative studies: varieties and role in legal sciences // The Scientific Heritage. 2021. No. 70-4(70). pp. 33-35.
3. U. S. Code // Legal Information Institute. URL: https://www.law.cornell.edu/uscode/text/18/1030 (date of application 18.11.2022).
4. The Criminal Code of the Russian Federation: Federal Law No. 63-FZ of 13.06.1996 // Collection of Legislation of the Russian Federation. 1996. No. 25. St. 2954.
5. Fraud Act 2006 // The Crown Prosecution Service. URL: https://www.cps.gov.uk/legal-guidance/fraud-act-2006 (date of application 19.11.2022).
6. Criminal Code // Justice Laws Website. URL: https://laws-lois.justice.gc.ca/eng/acts/c-46/page-54.html#h-122702 (date of application 20.11.2022).
7. Crimes Act 1961 // New Zealand Legislation. URL: https://legislation.govt.nz/act/public/1961/0043/latest/DLM330422.html (date of application 20.11.2022).