§5 АДМИНИСТРАТИВНОЕ И МУНИЦИПАЛЬНОЕ ПРАВО И ПРОБЛЕМЫ ИНФОРМАТИЗАЦИИ

Фролов М.Д.

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА МОШЕННИЧЕСТВО В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ПО ЗАКОНОДАТЕЛЬСТВУ СТРАН СЕВЕРНОЙ И ЮЖНОЙ АМЕРИКИ, ОКЕАНИИ, АЗИИ И АФРИКИ

Аннотация. *Автор подробно рассматривает такие аспекты темы как особенности установления уголовной ответственности за мошенничество в сфере компьютерной информации по законодательству стран Северной и Южной Америки, Океании, Азии и Африки. Это имеет непосредственное практическое значение, поскольку транснациональный характер компьютерного мошенничества предполагает необходимость взаимодействия с правоохранительными органами и правовыми системами других государств. Такое сотрудничество представляется возможным только при условии отчетливого понимания национальных особенностей установления и реализации ответственности за данное преступление. Автором использованы следующие методологические основы: совокупность общенаучных и специальных методов познания социально-правовой действительности. Методологический базис исследования представлен диалектическим методом с присущими ему требованиями объективности, всесторонности, историзма, конкретности истины. Из числа общенаучных методов исследования используются методы анализа, синтеза, сравнения, измерения. В качестве частнонаучных методов использован формально юридический и сравнительно-правовой метод . Основными признаками анализируемого преступления довольно часто признается групповой характер его совершения. В отдельных странах отягчающими обстоятельствами выступают использование лицом своего доверительного (служебного) положения или информационно-телекоммуникационной сети Интернет, малолетний или престарелый возраст потерпевшего. Следует особо отметить, что в изменение, уничтожение или блокирование компьютерной информации иногда выступает не конструктивным, а квалифицирующим признаком компьютерного мошенничества. Статья предназначена для студентов, аспирантов, преподавателей, сотрудников правоохранительных органов, практикующих юристов, а также для всех, кто интересуется проблемами соответствующей тематики.*

Ключевые слова: *уголовное право, уголовная ответственность, компьютерное мошенничество, Интернет, мошенничество, информационные технологии, компьютерная информация, Америка, Азия, Африка.*

Review. *The author discusses such aspects of the topic as the peculiarities of criminal liability for computer fraud in the legislation of the countries of North and South America, Oceania, Asia and Africa. The topic is of a practical importance, since the transnational character of computer fraud presupposes the necessity to interact with law enforcement bodies and legal systems of other states. Such cooperation is only possible provided that there is a clear understanding of national peculiarities of liability imposition. The author applies the set of general scientific and special methods of cognition. The methodology of the research is based on the dialectical method with its requirements for objectivity, comprehensiveness, historicism and clarity of truth. The author applies the methods of analysis, synthesis, comparison and measurement. The formal-legal and the comparative-legal methods are used as special scientific methods. The group character of an analyzed crime is often recognized as its main feature. In certain countries the abuse of authority, the misuse of the Internet, and minor or senile age of the aggrieved person can be considered as matters of aggravation. It should be mentioned that sometimes change, destruction of blocking of computer data serves not as a constructive, but as a qualifying feature of computer fraud. This article can be used by students, postgraduates, lecturers, law enforcement officers and practicing lawyers, and by all interested in this subject.*

Keywords: *information technologies, fraud, Internet, computer fraud, criminal liability, criminal law, computer data, America, Asia, Africa.*

DOI: 10.7256/1999-2807.2015.11.16911

Обращаясь к проблеме уголовной ответственности за мошенничество в сфере компьютерной информации нельзя оставить без внимания зарубежный опыт противодействия данному виду преступной деятельности. Прежде всего это имеет непосредственное практическое значение, поскольку транснациональный характер компьютерного мошенничества предполагает необходимость взаимодействия с правоохранительными органами и правовыми системами других государств. Такое сотрудничество представляется возможным только при условии отчетливого понимания национальных особенностей установления и реализации ответственности за данное преступление. Кроме того, сравнительно-правовое исследование всегда позволяет по-иному взглянуть на отечественное законодательство, способствует выявлению его слабых и сильных сторон, а также построению аргументированных предложений по его дальнейшему совершенствованию.

В феврале 2013 года Управление Организации Объединенных Наций по наркотикам и преступности (UNODC) подготовило доклад по результатам комплексного изучения киберпреступности Comprehensive Study on Cybercrime 2013. Согласно выводам UNODC из числа исследованных стран уголовно-правовое противодействие компьютерному мошенничеству в 40% реализуется посредством применения общих положений о преступлениях против собственности, еще в 40% посредством применения специальных норм о мошенничестве в сфере компьютерной информации и в 15% странами используется так называемый комбинированный подход, основанный на квалификации действий лиц по совокупности преступлений об общеуголовном мошенничестве и против компьютерной информации.

Во многом по причине самой структуры своей правовой системы значительный материал для анализа по проблеме уголовной ответственности за мошенничество в сфере компьютерной информации содержит уголовное законодательство Соединенных Штатов Америки. Следует отметить, что основой для развития законодательства об ответственности за совершение компьютерных преступлений на уровне отдельных штатов явился Закон о компьютерном мошенничестве и злоупотреблениях с их использованием (Computer fraud and abuse act (CFAA), принятый в 1986 году. В §1030 Свода законов США мошенничество с использованием компьютера определяется как доступ к компьютерной информации, осуществляемый с мошенническими намерениями, или использование компьютера с целью получения чего бы то ни было ценного посредством мошенничества.

Раздел 5 «Criminal offenses» (Преступления) Свода законов штата Арканзас в подразделе 4 «Offenses against property» (Преступления против собственности) выделяет главу 41 «Computer-related crimes» (Преступления, связанные с использованием компьютеров). Согласно § 5-41-103 «Computer fraud» (Компьютерное мошенничество) Свода законов штата Арканзас лицо совершает компьютерное мошенничество в случае, если оно, используя доступ к компьютеру, компьютерной системе или сети, похищает деньги или иное имущество путем обмана или ложного представительства. Законодатель штата Арканзас относит компьютерное мошенничество к фелонии класса D. В соответствии с пунктом 4 § 5-4-401 «Sentence» Свода законов штата Арканзас лицо признанное виновным в совершении такого преступления подлежит наказанию в виде лишения свободы на срок до 6 лет.

Свод законов штата Луизиана уголовную ответственность за компьютерное мошенничество устанавливает в §73.5 «Computer fraud» (Компьютерное мошенничество). Обязательным конструктивным признаком данного состава выступает как использование лицом компьютера, информационной сети или системы, так и обман (ложное представительство). Согласно законодательству штата Луизиана компьютерное мошенничество наказывается штрафом до 10 тысяч долларов США либо лишением свободы на срок до 5 лет или обоими этими видами наказания.

Примечательной особенностью законодательства штата Луизиана является специальное определение в качестве отягчающего обстоятельства использование лицом при совершении компьютерного преступления информационно-телекоммуникационной сети Интернет. В соответствии с пунктом «а» § 73.9 Свода законов штата Луизиана использование лицом Интернета при преступном посягательстве в отношении лица или против собственности влечет назначение дополнительного наказания в виде лишения свободы на срок не менее 1 года.

Практически идентичное положение об ответственности за компьютерное мошенничество предусмотрено в главе 45 «Computer crimes and identity theft» (Компьютерные преступления и хищения персональных данных) §97-45-3 «Computer fraud; penalties» Свода законов штата Миссисипи. Вместе с тем, в отличие от законодателя Луизианы данная статья дифференцирует ответственность виновного лица в зависимости от размера причиненного ущерба потерпевшему. Так, основной состав компьютерного мошенничества наказывается штрафом в размере до 1 тысячи долларов США либо лишением свободы на срок не более 6 меся-

DOI: 10.7256/1999-2807.2015.11.16911

цев, либо обоими этими видами наказания. В тех же случаях, когда ущерб превышает 500 долларов США, виновное лицо подлежит наказанию в виде штрафа до 10 тысяч долларов США либо лишения свободы на срок до 5 лет, либо обоих этих видов наказания.

По уголовному законодательству Западной Виржинии компьютерное мошенничество наказывается штрафом до 10 тысяч долларов США либо лишением свободы на срок до 10 лет или обоими этими видами наказания (§61-3C-4).

Свод законов штата Нью-Йорк положения о мошенничестве в сфере компьютерной информации предусматривает в разделе «К» «Offenses involving fraud» (Преступления, связанные с мошенничеством (обманом). В соответствии со статьями 190.78 – 190.80 лицо подлежит уголовной ответственности за неправомерное использование персональной информации (personal identifying information), представленной в любой форме с целью хищения имущества другого лица. Размер хищения также влияет на квалификацию и ответственность виновного: если размер похищенного не превышает 500 долларов США содеянное признается мисдиминором класса «А» (ст. 190.78) и наказывается лишением свободы на срок до 1 года; если размер похищенного превышает 500 долларов США содеянное признается фелонией класса «Е» (ст. 190.79) и наказывается лишением свободы на срок до 4 лет; если размер похищенного превышает 2 тысячи долларов США содеянное признается фелонией класса «D» (ст. 190.80) и наказывается лишением свободы на срок до 7 лет.

Уголовный кодекс Канады в ст. 403 устанавливает ответственность за использование персональных данных в целях хищения чужого имущества. В соответствии с санкцией лицо, признанное виновным в совершении данного преступления, подлежит наказанию в виде лишения свободы на срок до 10 лет. В соответствии со ст. 402.1 под персональными данными лица понимается следующая информация: отпечатки пальцев, имя, адрес, дата рождения, собственноручная подпись, электронная подпись, цифровая подпись, имя пользователя, номер кредитной карты, номер дебетовой карты, номер финансового счета, номер паспорта, номер полиса социального страхования, номер медицинской страховки, номер водительского удостоверения или пароль.

В уголовных законодательствах стран Южной Америки мошенничество в сфере компьютерной информации, как правило, специально не выделяется. В связи с этим, правоохранительными органами этих государств подобные деяния квалифицируются по совокупности преступлений. Так, Хосе Луис Акунья Гонсалес, оценивая современное состояние преступности в сфере компьютерного мошенничества в Чили, отмечает, что специфическое поведение, связанное с компьютерным мошенничеством, под которым могут пониматься любые информационные махинации, осуществляемые хакерами или третьими лицами с помощью данных, полученных обманным путем, и причиняющие имущественный ущерб владельцу этих данных, не квалифицируется ни нашим Уголовным кодексом, ни специальными законами, определяя такое поведение как информационное вредительство и в соответствии с общими положениями Уголовного кодекса, например, как мошенничество, присвоение имени или преступление в сфере интеллектуальной собственности[1].

Уголовный кодекс Австралии в ст. 133.1 раскрывает общее понятие обмана (deception***)***, под которым предлагается понимать не только введение в заблуждение другого человека, но и совершение действий, связанных с использованием компьютерной информации, которые виновное лицо не имело право совершать. В соответствии со ст.134.1 «Получение имущества путем обмана» (Obtaining property by deception) лицо, совершившее хищение чужого имущества путем обмана, наказывается лишением свободы на срок до 10 лет.

Уголовный кодекс Новой Зеландии ответственность за компьютерное мошенничество предусматривает в ст. 249 «Использование компьютерной системы в бесчестных целях» (Accessing computer system for dishonest purpose). Примечательной особенностью анализируемой нормы является то обстоятельство, что в части 1 законодатель устанавливает ответственность за оконченное преступление, которое наказывается лишением свободы на срок до 7 лет, а в части 2 за совершение тех же действий, чтобы получить чужое имущества – наказывается лишением свободы на срок до 5 лет. Следует отдельно отметить, что в отличие от многих других стран, норма о компьютерном мошенничестве в УК Новой Зеландии располагается не в группе преступлений против собственности, а в главе о преступлениях, связанных с компьютерами (Crimes involving computers).

Исследование стран Азии показало, что распространенной моделью установления уголовной ответственности за компьютерное мошенничество является закрепление ссылочных уголовно-правовых норм. Так, Закон о неправомерном использовании компьютерных технологий Сингапура (Computer misuse act (CMA) в целом основывается на положениях законодательства о киберпреступности Великобритании. В соответствии со ст. 4 данного закона лицо подлежит уголовной ответственности за доступ к компьютерным данным с намерением совершения или содействия совер-

DOI: 10.7256/1999-2807.2015.11.16911

шению преступления (Access with intent to commit or facilitate commission of offence). Структура данной статьи своеобразна – в части 2 оговаривается, что она распространяется только на те деяния (связанные с посягательством на собственность, мошенничеством, подлогом или причинением личного (физического) вреда), наказание за которые составляет не менее 2 лет лишения свободы. Согласно части 3 лицо, признанное виновным в совершении подобного преступления наказывается лишением свободы на срок до 10 лет со штрафом в размере до 50 тысяч сингапурских долларов или без такового.

Аналогичный подход реализован в Законе о неправомерном использовании компьютерных технологий Малайзии (Malaysia computer crime act). Принципиальным отличием является лишь то, что законодатель Малайзии не устанавливает каких-либо ограничений по минимальному сроку наказуемости общеуголовного преступления.

Уголовный кодекс Китая в ст. 287 ограничивается лишь общим положением о том, что использование компьютера для завладения деньгами путем мошенничества или их хищения, для взяточничества и нецелевого использования общественных средств, для завладения путем хищения государственной тайной и совершения иных преступлений, наказывается согласно соответствующим статьям данного кодекса.

Отличный от других подход избрал законодатель Японии. Согласно ст. 246-2 УК Японии за компьютерное мошенничество лицо наказывается лишением свободы на срок до 10 лет, если оно «изготовило фальшивые электромагнитные записи, свидетельствующие о приобретении, изменении или потере имущественных прав, путем внесения в компьютер ложных сведений или команд либо использовало фальшивые электромагнитные записи в ходе деловых операций, и получило в результате этого незаконный доход либо способствовало получению незаконного дохода третьим лицом».

Специальные нормы о компьютерном мошенничестве нашли свою регламентацию и в правовых системах стран Африки. Так, ответственность за компьютерное и телекоммуникационное мошенничество (Computer and telecommunications swindle) предусмотрена ст. 407 Уголовного кодекса Анголы. Похожие нормы о мошенничестве в сфере компьютерной информации содержатся в ст. 15 Закона о киберпреступности и компьютерных преступлениях Ботсваны (Cybercrime and computer related crimes act), ст. 173 Закона об информации и коммуникациях Гамбии (Information and Communications Act), ст. 122 Закона об электронных операциях Ганы (Electronic Transactions Act), ст. 73 Закона о кибербезопасности и киберпреступности Камеруна (Cyber security and cybercrime act), ст.84В Закона об информации и коммуникациях Кении (Information and Communications Act), ст. 707 Уголовного кодекса Эфиопии, ст.87 Закона об электронных коммуникациях и операциях Южной Африки (Electronic communications and transactions act).

В целом анализ зарубежного законодательства позволяет согласиться с выводами UNODC – в современных условиях страны по-разному подходят к решению вопроса установления уголовной ответственности за мошенничество в сфере компьютерной информации. Неодинаковым является и определение содержания общественных отношений, которым причиняется вред при совершении данного преступления. Так, в одних странах мошенничество в сфере компьютерной информации рассматривается как преступление против собственности, в других – как преступление, которое прежде всего посягает на установленный порядок использования компьютерных данных, компьютерного оборудования и систем.

В абсолютном большинстве исследуемых зарубежных стран основным критерием дифференциации уголовной ответственности за мошенничество в сфере компьютерной информации выступает размер похищенного имущества. Вместе с тем, проведенное исследование позволило выявить и иные законодательные решения. Квалифицирующими признаками анализируемого преступления довольно часто признается групповой характер его совершения (в составе группы лиц по предварительному сговору или организованной группы). В отдельных странах отягчающими обстоятельствами выступают использование лицом своего доверительного (служебного) положения или информационно-телекоммуникационной сети Интернет, малолетний или престарелый возраст потерпевшего. Следует особо отметить, что в некоторых странах изменение, уничтожение или блокирование компьютерной информации выступает не конструктивным, а квалифицирующим признаком компьютерного мошенничества.

Библиография:

1. Хосе Луис Акунья Гонсалес. Современное состояние преступности в сфере компьютерного мошенничества в Чили // Юридическая техника. 2014. №8
2. Степанов-Егиянц В.Г. Понятийно-терминологические основы безопасного обращения компьютерной информации в уголовно-правовом аспекте // Право и политика. – 2015. – 4. – С. 592 – 599. DOI: 10.7256/1811-9018.2015.4.14776.

DOI: 10.7256/1999-2807.2015.11.16911

3. Букалерова Л.А., Остроушко А.В. Специфика уголовной, административной, гражданско-правовой ответственности за информационные правонарушения в системе публичного управления // NB: Административное право и практика администрирования. – 2015. – 1. – С. 81 – 94. DOI: 10.7256/2306-9945.2015.1.14109. URL: http://www.e-notabene.ru/al/article_14109.html
4. Д.К. Чирков, А.Ж. Саркисян Преступность в сфере высоких технологий: тенденции и перспективы // Национальная безопасность / nota bene. – 2013. – 1. – С. 20 – 26. DOI: 10.7256/2073-8560.2013.01.3.
5. Карчевский Н.В. Основные направления обеспечения уголовно-правовой охраны информационной безопасности // Право и политика. – 2015. – 2. – С. 180 – 188. DOI: 10.7256/1811-9018.2015.2.8115.

References (transliterated):

1. Khose Luis Akun'ya Gonsales. Sovremennoe sostoyanie prestupnosti v sfere komp'yuternogo moshennichestva v Chili // Yuridicheskaya tekhnika. 2014. №8
2. Stepanov-Egiyants V.G. Ponyatiino-terminologicheskie osnovy bezopasnogo obrashcheniya komp'yuternoi informatsii v ugolovno-pravovom aspekte // Pravo i politika. – 2015. – 4. – C. 592 – 599. DOI: 10.7256/1811-9018.2015.4.14776.
3. Bukalerova L.A., Ostroushko A.V. Spetsifika ugolovnoi, administrativnoi, grazhdansko-pravovoi otvetstvennosti za informatsionnye pravonarusheniya v sisteme publichnogo upravleniya // NB: Administrativnoe pravo i praktika administrirovaniya. – 2015. – 1. – C. 81 – 94. DOI: 10.7256/2306-9945.2015.1.14109. URL: http://www.e-notabene.ru/al/article_14109.html
4. D.K. Chirkov, A.Zh. Sarkisyan Prestupnost' v sfere vysokikh tekhnologii: tendentsii i perspektivy // Natsional'naya bezopasnost' / nota bene. – 2013. – 1. – C. 20 – 26. DOI: 10.7256/2073-8560.2013.01.3.
5. Karchevskii N.V. Osnovnye napravleniya obespecheniya ugolovno-pravovoi okhrany informatsionnoi bezopasnosti // Pravo i politika. – 2015. – 2. – C. 180 – 188. DOI: 10.7256/1811-9018.2015.2.8115.

DOI: 10.7256/1999-2807.2015.11.16911