КОМПАРАТИВИСТСКИЕ ИССЛЕДОВАНИЯ УГОЛОВНОГО ПРАВА, КРИМИНОЛОГИИ И УГОЛОВНО-ИСПОЛНИТЕЛЬНОГО ПРАВА

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ПО ЗАКОНОДАТЕЛЬСТВУ КИТАЙСКОЙ НАРОДНОЙ РЕСПУБЛИКИ: СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ

РУСКЕВИЧ Евгений Александрович, доцент кафедры уголовного права Московского университета МВД России им. В. Я. Кикотя, кандидат юридических наук
117437, Россия, г. Москва, ул. Академика Волгина, 12
E-mail: russkevich@mail.ru

Расширение экономических связей между Россией и Китаем, равно как и поддержание крепких партнерских отношений на международной арене, обуславливают значительный интерес к сравнительному исследованию законодательств двух стран. При этом существенный теоретико-прикладной потенциал имеет познание китайского опыта законодательного определения компьютерных преступлений. В Уголовном кодексе Китая, как и в России, первые нормы об ответственности за преступления в сфере компьютерной информации появились в 1997 г. Вместе с тем в последующем «китайская модель» противодействия киберпреступности неоднократно совершенствовалась и в настоящее время считается одной из наиболее сбалансированных и эффективных.

Цель работы состоит в проведении исследования уголовной ответственности за преступления в сфере компьютерной информации в Китайской Народной Республике и в разработке на этой основе предложений по совершенствованию гл. 28 УК РФ. Реализация указанной цели достигалась путем оценки состояния уголовного законодательства Китая в части регламентации ответственности за посягательства на компьютерную информацию, а также средства ее автоматизированной обработки, хранения и передачи.

Исследование основано на применении сравнительно-правового метода. Также использованы общенаучные и специальные методы.

Выводы: 1) имея с Россией общую точку отсчета в построении уголовно-правового механизма противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий, Китай реализовал более сложную модель их криминализации; 2) китайская модель уголовно-правового противодействия киберпреступности развивалась в три этапа: защита критической информационной инфраструктуры; расширение защиты информационных ресурсов частных лиц; установление ответственности провайдеров и виртуальных пособников; 3) применительно к отечественной проблематике уголовно-правового противодействия киберпреступности наибольшим теоретико-прикладным значением обладают положения уголовного законодательства Китая об ответственности провайдеров и лиц, использующих интернет-ресурсы для распространения криминогенной информации и оказания неперсонифицированной помощи для совершения преступлений.

Ключевые слова: уголовное право, компьютерные преступления, информационно-коммуникационные технологии, уголовное законодательство Китая.

CRIMINAL LIABILITY FOR COMPUTER CRIMES UNDER THE LAWS OF THE CHINESE PEOPLE'S REPUBLIC: COMPARATIVE-LEGAL ANALYSIS

E. A. RUSSKEVICH, associate professor at the Department of criminal law of the Kikot Moscow University of the Ministry of Internal Affairs of the Russian Federation, candidate of legal sciences
12, Akademik Volgin st., Moscow, Russia, 117437
E-mail: russkevich@mail.ru

The expansion of economic ties between Russia and China, as well as the maintenance of strong partnership relations in the international arena, are of considerable interest to a comparative study of the two countries' legislations. At the same time, the significant theoretical and applied potential has knowledge of the Chinese experience in legislative definition of computer crimes. In the Criminal Code of China, as in Russia, the first rules on liability for crimes in the field of computer information appeared in 1997. At the same time over the past years, the "Chinese model" of countering cybercrime has been repeatedly improved and is now considered as one of the most balanced and effective.

The purpose of the work is to conduct a study of criminal liability for crimes in the field of computer information in the People's Republic of China and developing on this basis some proposals for improving Chapter 28 of the Criminal Code. The implementation of this goal is achieved by assessing the state of criminal law in China regarding regulation of liability for computer information infringement, as well as means of its automated processing, storage and transmission.

The study is mainly based on the application of a comparative-legal method. At the same time, general scientific and special methods (analysis, synthesis, induction, formal-legal, abstract-logical, etc.) are also used.

Conclusions: 1) possessing a common reference point with Russia (1997) in building a criminal legal mechanism to counteract crimes committed by means of information and communication technologies, China has implemented a more complex model of their criminalization; 2) the Chinese model of the criminal legal counteraction to cybercrime are developed in three stages: the first stage is a critical information infrastructure protection (1997), the second stage is the protection of individuals' information resources (2009) and the third stage is establishing responsibility for providers and virtual collaborators (2015); 3) with reference to the domestic problems of criminal legal counteraction of cybercrime, the provisions of China's criminal law on the liability of providers and persons using Internet resources for dissemination of criminal information and rendering non-personalized assistance for committing crimes, which have the greatest theoretical and applied significance.

Keywords: criminal law, computer crimes, information and communication technologies, criminal law of China.

DOI: 10.12737/art.2018.5.15

Китай является одним из ведущих государств с миллиардным населением и второй по значимости экономикой мира. В отечественной юридической науке изучению развития китайского права всегда уделялось значительное внимание¹. Обращаясь к анализу правовой системы Китая, П. В. Трощинский обоснованно призывает учитывать своеобразие китайского права, правовой культуры и правосознания его граждан, которые были сформированы под глубоким влиянием нравственного учения великого Конфуция².

При этом В. В. Севальнев справедливо делает вывод, что правовую систему Китая нельзя полностью отнести к романо-германской (континентальной) системе, она является смешанной и представляет собой симбиоз древних правовых традиций и современного законодательства, которое основано на идеях «социализма с китайской спецификой», принципах романо-германского права, при этом она подвергалась серьезному влиянию правовой модели СССР³.

Как и в России, до 1997 г. в уголовном законодательстве Китая не было специальных положений об ответственности за посягательства на компьютерную информацию, а также средства ее автоматизированной обработки или передачи. Суды разреша-

ли возникающие проблемные ситуации на основе традиционных составов преступлений, прибегая, как правило, к крайне расширительному толкованию положений уголовного закона. Так, в 1986 г. состоялось известное решение по делу Чена, которое считается первым приговором по киберпреступлению в Китае. Чен, работая операционистом в банке, воспользовался служебным доступом к информационной системе банка и изменил сведения о балансе принадлежащего ему банковского счета. Вынося обвинительный приговор, суд применил положения УК Китая о краже⁴.

Данное решение было неоднозначно воспринято в научном сообществе Китая и вызвало бурную полемику по поводу правильности применения положений о краже. Противники вынесенного решения указывали на то, что Чен в сущности никакого имущества не изымал, им были неправомерно модифицированы сведения в информационной системе банка, и поэтому ответственность за кражу он нести не может⁵. Другие ссылались на то, что расширительное толкование состава общеуголовной кражи позволяет распространить его и на действия, совершенные с использованием современных информационных систем кредитно-финансовых учреждений, поскольку умысел виновного был направлен именно на получение материальной выгоды⁶. Так или иначе практически все специалисты соглашались в одном — уголовное законодательство Китая должно быть дополнено специальными положениями об ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий.

¹ См., например: Гудошников Л. М. Исследование политико-юридических проблем Китая в ИДВ РАН // Проблемы Дальнего Востока. 2005. № 6. С. 31—42; Трощинский П. В. Право Китая в зеркале российской науки // Государство и право. 2018. № 1. С. 82—95; Лузянин С. Г., Трощинский П. В., Суходолов Я. А. Особенности правового регулирования борьбы с преступностью в Китае // Всероссийский криминологический журнал. 2016. Т. 10. № 4. С. 812—824.

² См.: Трощинский П. В. К вопросу о традиционных взглядах на право в китайском обществе // Вестник Университета им. О. Е. Кутафина. 2016. № 3. С. 146.

³ См.: Севальнев В. В. Правовое регулирование противодействия коррупции в Китае // Журнал зарубежного законодательства и сравнительного правоведения. 2018. № 2. С. 70.

⁴ Пример приведен по: Qianyun Wang. A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe. Rotterdam, 2016. P. 42.

⁵ См.: Chen Lihua. The Discussion on Computer Crime and its Legislation // Legal Science. 1990. No. 1. P. 42.

⁶ См.: Ma Qiufeng. The Concept of Computer Crime // China Academic Journal Electronic Publishing House. 1992.

УК Китая (в первоначальной редакции 1997 г.) предусматривал три специальные статьи, связанные с компьютерными преступлениями:

ст. 285 регламентировала ответственность за неправомерный доступ к информационным ресурсам, связанным с деятельностью органов государственной власти, иных особо важных отраслей и обеспечением обороноспособности страны (т. е. к «объектам критической информационной инфраструктуры» в терминологии отечественного уголовного законодательства);

в соответствии со ст. 286 уголовно наказуемыми считались: 1) неправомерное вмешательство в работу средств автоматической обработки данных и 2) изготовление и распространение вредоносных компьютерных программ;

ст. 287 не предусматривала самостоятельного уголовно-правового запрета и указывала на то, что «традиционные посягательства, совершаемые с использованием компьютерной техники, такие как мошенничество, кража, государственная измена и др., наказываются в соответствии с общими положениями уголовного законодательства об ответственности за данные преступления»⁷.

Вместе с тем реализованная модель уголовной ответственности за посягательства на отношения, связанные с обеспечением безопасности компьютерных данных и систем, вызвала критику у представителей китайской науки, суть которой сводилась к тому, что указанные нормы не охватывают ситуацию неправомерного доступа к компьютерным системам частных лиц (граждан и организаций) при условии, что это никак не повлияло на работу средств автоматизированной обработки данных⁸.

Действительно, при буквальном толковании ст. 286 УК Китая (в ред. 1997 г.) следует сделать вывод, что она могла быть применена только в тех случаях, когда неправомерное вмешательство в работу компьютерной системы повлекло ухудшение ее функционирования. Если же был осуществлен доступ без замедления работы системы или деструктивного воздействия на сами компьютерные данные, содеянное не могло быть признано преступлением, поскольку ст. 285 заведомо устанавливала ответственность только за неправомерный доступ к информационным ресурсам государственного и общественного значения.

В 2009 г. были внесены первые поправки в уголовное законодательство Китая, связанные с ответственностью за преступления, совершаемые с использованием информационно-коммуникационных технологий. Так, ст. 285 УК Китая была дополнена

ч. 2, устанавливающей ответственность за неправомерные уничтожение, повреждение или модификацию данных, хранящихся в информационной системе частных лиц, и ч. 3, криминализирующей распространение программно-технических средств, заведомо предназначенных для совершения преступлений, предусмотренных ч. 1 и 2 данной статьи.

В целом данные изменения явились ответом на все возрастающее значение компьютерных технологий в повседневной жизни граждан и деятельности хозяйствующих субъектов Китая.

В 2015 г. была принята девятая поправка к УК Китая, которая дополнила его тремя новыми составами преступлений в сфере компьютерной информации:

в соответствии со ст. 286А была установлена ответственность провайдеров за неисполнение решений контролирующих органов по блокированию соответствующих интернет-ресурсов и удалению запрещенной информации;

ст. 287А установила ответственность за использование интернет-ресурсов для распространения информации (обучения) о способах совершения преступлений;

в соответствии со ст. 287В было криминализовано виртуальное содействие совершению киберпреступлений⁹.

Указанные изменения стали следствием реализации курса государства на борьбу с возрастающей криминализацией виртуального пространства, в том числе в части создания лицами специализированных информационных ресурсов, предназначенных для обмена информацией и программно-техническими средствами для совершения преступлений¹⁰.

Таким образом, действующее законодательство Китая содержит следующие уголовно-правовые нормы об ответственности за компьютерные преступления: неправомерный доступ (ст. 285), неправомерное вмешательство в работу (функционирование) компьютерной системы (ст. 286), неисполнение решения контролирующего органа о блокировании интернет-ресурса или удалении информации (ст. 286А), использование интернет-ресурсов для распространения информации о совершении преступлений (криминальной информации) (ст. 287А) и содействие совершению киберпреступлений (ст. 287В). При этом ст. 287 УК Китая представляет собой гиперссылочную уголовно-правовую норму, легитимирующую применение традиционных положений китайского уголовного законодательства к случаям совершения

⁹ URL: <http://www.fmprc.gov.cn/ce/cgvienna/eng/dbtyw/jdwt/crimelaw/t209043.htm> (дата обращения: 21.05.2018).

¹⁰ См.: Li Huaisheng. The Evolution of Cybercrime in Three Generations of the Information Network and the Law-Making // Legal Forum. 2015. No. 4. P. 94; Yu Zhigang. The Criminalization of Training Hackers in Cyberspace // Law Edition Journal of Yunnan University. 2015. No. 1. P. 86.

⁷ URL: <http://www.fmprc.gov.cn/ce/cgvienna/eng/dbtyw/jdwt/crimelaw/t209043.htm> (дата обращения: 21.05.2018).

⁸ См.: Zhao Bingzhi, Yu Zhigang. Computer Crime and the Response from Legislation and Legal Theory // China Legal Science. 2001. No. 1. P. 149.

иных общеуголовных преступлений с использованием современных информационно-коммуникационных технологий.

Цяньюнь Ван справедливо отмечает, что по смыслу ст. 285 УК Китая уголовно наказуемым является противоправное преодоление средств программно-технической защиты информации (взлом сам по себе, так называемое чистое хакерство), совершенное только в отношении объектов критической информационной инфраструктуры. Взлом компьютерной системы частных лиц без последующего воздействия на компьютерную информацию (ее уничтожение, повреждение, блокирование или модификацию) не является преступлением¹¹.

Нельзя не отметить очевидную близость в данном вопросе законодательства Китая отечественной уголовно-правовой норме об ответственности за неправомерный доступ к компьютерной информации (ст. 272 УК РФ), которая, как известно, в ряду обязательных конструктивных признаков состава также называет общественно опасные последствия в виде уничтожения, блокирования, модификации или копирования компьютерной информации.

Вместе с тем, в отличие от китайской модели, УК России предусматривает обязательность последствий (причинение вреда) и для неправомерного доступа к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации (ч. 2 ст. 274¹). При этом вред как конструктивный признак состава преступления, предусмотренного ч. 2 ст. 274¹ УК РФ, не конкретизирован, т. е. является оценочным признаком. Системное толкование позволяет предположить, что таковыми являются все те же последствия в виде уничтожения, блокирования, модификации или копирования информации, содержащейся в критической информационной инфраструктуре.

Полагаем, что подход законодателя Китая в части уголовно-правовой охраны критической информационной инфраструктуры государства является более предпочтительным. Особая значимость таких ресурсов для обеспечения обороноспособности государства, общественной безопасности и поддержания общественного порядка позволяет сделать вывод о необходимости признания преступлением самих действий по их компьютерной атаке.

Отдельно следует уделить внимание китайскому подходу к определению «вредоносная компьютерная программа». В своей работе Цяньюнь Ван отмечает, что применение ч. 3 ст. 285 УК Китая вызвало ряд трудностей в части квалификации действий с так называемыми компьютерными программами двойного назначения. Такое программное обеспечение предназначено для тестирования специалистами компьютерных систем защиты информации,

однако может быть использовано и при совершении преступлений¹².

В решении данной проблемы руководящее значение имеют разъяснения Верховного суда КНР 2011 г., согласно которым «вредоносная компьютерная программа» должна соответствовать следующим обязательным критериям: 1) получение компьютерной информации и воздействие на средства автоматизированной обработки данных должны выступать основными функциями вредоносной компьютерной программы; 2) вредоносная компьютерная программа должна обладать возможностью (функционалом) по преодолению средств программно-технической защиты компьютерных данных и систем; 3) работа вредоносной компьютерной программы предполагает, что доступ к компьютерной информации или вмешательство в работу средств автоматизированной обработки данных имеет несанкционированный характер, т. е. осуществляется без надлежащих на то полномочий¹³.

Выделенные Верховным судом КНР признаки позволяют решить многие проблемы квалификации преступления, связанного с оборотом вредоносных компьютерных программ. Вместе с тем указанное толкование оставляет отдельные вопросы относительно содержания признака вредоносности. Так, например, китайская модель не позволяет признать вредоносной компьютерную программу, которая заведомо предназначена для автоматизированного изготовления самих компьютерных вирусов (так называемый конструктор вирусов).

Деяние, предусмотренное ст. 285А УК Китая, имеет очевидное сходство с положениями российского законодательства об ответственности за неисполнение оператором связи, оказывающим услуги по предоставлению доступа к сети Интернет, обязанности по ограничению доступа к информации, доступ к которой должен быть ограничен на основании сведений, полученных от федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций (ст. 13.34 КоАП РФ). Вместе с тем необходимо отметить, что состав преступления, предусмотренный ст. 285А УК Китая, обладает материальной конструкцией и в качестве обязательных признаков называет следующие альтернативные последствия: 1) если неисполнение решение провайдером привело к «массовому распространению» запрещенной информации и 2) повлекло наступление тяжких последствий.

¹² См.: *Qianyun Wang*. Op. cit. P. 56.

¹³ Interpretations of Several Issues on the Application of Law in Handling Criminal Cases about Endangering the Security of Computer Information Systems. 2011. No. 19. URL: <http://www.scio.gov.cn/xwfbh/qyxwfbh/document/1004368/1004368.htm>. (дата обращения: 21.05.2018).

¹¹ См.: *Qianyun Wang*. Op. cit. P. 55.

Несмотря на использование китайским законодателем оценочных признаков, которые закономерно вызовут определенные затруднения на практике, само решение о криминализации таких действий следует признать положительным. В этом отношении отечественное законодательство выглядит несогласованным и непоследовательным, поскольку, устанавливая административную ответственность за простое бездействие провайдера по удалению запрещенного контента или блокированию криминогенного интернет-ресурса, оно не определяет ответственность поставщика связи в случаях, когда такое неисполнение привело к тяжким последствиям, выразившимся, например, в гибели человека, массовых беспорядках, дезорганизации деятельности органов государственной власти и т. д.

В статье 287А законодатель Китая весьма удачно решает проблему ответственности за виртуальное содействие в совершении преступлений без признаков соучастия. Как известно, в отечественной доктрине уголовного права масштабное распространение безадресного подстрекательства и предлагаемой по принципу «до востребования» помощи в совершении компьютерных преступлений позволило отдельным специалистам сделать вывод о необходимости переосмысления некоторых общетеоретических положений института соучастия. Так, А. Ю. Чупрова пишет, что особенностью подстрекательских действий в сети Интернет является то, что умысел лица не персонифицирован, его призыв к совершению преступления обращен к неопределенно большому кругу лиц. Кто найдет предложение заслуживающим внимания и одобрения и реализует его на практике, автору прокламации неизвестно¹⁴.

Полагаем, что попытки переосмысления аксиоматического положения о невозможности привлечения к ответственности за так называемое абстрактное соучастие вряд ли являются оправданными. Подстрекательством может быть признано склонение другого лица к совершению конкретного преступления, а не пробуждение абстрактных преступных устремлений или интереса к противоправному поведению. Недостаточно дать кому-то совет заняться кражами: для признания лица подстрекателем необходимо, чтобы оно подстрекнуло совершить определенную кражу путем объяснения выгод от преступления, умаления трудностей и опасности, с которыми сопряжено его выполнение¹⁵. В той же мере сказанное относится и к пособничеству. Современная судебная практика демонстрирует строгую приверженность данной концепции¹⁶.

¹⁴ См.: Чупрова А. Ю. Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции: дис. ... д-ра юрид. наук. М., 2015. С. 259.

¹⁵ См.: Курс российского уголовного права. Общая часть / под ред. В. Н. Кудрявцева, А. В. Наумова. М., 2001. С. 359.

¹⁶ См. апелляционные определения ВС РФ от 27 апреля 2017 г. по делу № 89-АПУ17-Зсп, от 4 июня 2015 г. по делу № 30-АПУ15-3.

Тенденция к расширительному толкованию подстрекательских и пособнических действий по делам о компьютерных преступлениях имеет свое объяснение — публичное размещение информации, склоняющей или облегчающей их совершение, объективно является общественно опасным и требует надлежащей оценки. Однако даже при решении самых злободневных проблем нельзя законность приносить в жертву «социальной необходимости», произвольно расширяя пределы действия уголовного закона. Полагаем, что отечественному законодателю необходимо обратить более пристальное внимание именно на ст. 287А УК Китая, которая в рамках специальной нормы устанавливает ответственность за виртуальное содействие в совершении преступлений без признаков соучастия.

В статье 287В УК Китая криминализована деятельность пособника в совершении преступления посредством использования информационно-коммуникационных технологий. Таким образом, это как бы специальная норма о «виртуальном пособничестве». В отличие от ст. 287А, где лицо предоставляет вредоносные компьютерные программы «до востребования», в ст. 287В речь идет именно о содействии совершению конкретного преступления. Как справедливо подчеркивает Цяньюнь Ван, лицо должно достоверно знать о том, что пользователь, которому он оказывает помощь, намеревается совершить конкретное преступление (an actor obviously knows that the person to whom he providing help intends to commit a crime by means of a network)¹⁷.

С точки зрения отечественной теории уголовного права данное решение является примером так называемого избыточного законодательства. Появление подобной нормы не решает проблему уголовной ответственности лица, поскольку таковая уже была возможной с учетом общих положений о наказуемости пособнических действий.

Проведенное исследование позволяет сделать несколько значимых выводов общего характера. Имея с Россией общую точку отсчета (1997 г.) в построении уголовно-правового механизма противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий, Китай реализовал более сложную модель их криминализации.

Китайская модель уголовно-правового противодействия киберпреступности развивалась в три этапа: 1) защита критической информационной инфраструктуры (1997 г.); 2) расширение защиты информационных ресурсов частных лиц (2009 г.); 3) установление ответственности провайдеров и виртуальных пособников (2015 г.).

Применительно к отечественной проблематике уголовно-правового противодействия киберпреступности полагаем, что наибольшим теоретико-приклад-

¹⁷ См.: Qianyun Wang. Op. cit. P. 60.

ным значением обладают положения уголовного законодательства Китая об ответственности провайдеров и лиц, использующих интернет-ресурсы для

распространения криминогенной информации и оказания неперсонифицированной помощи для совершения преступлений.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

- Chen Lihua. The Discussion on Computer Crime and its Legislation // Legal Science. 1990. No. 1.
- Li Huaisheng. The Evolution of Cybercrime in Three Generations of the Information Network and the Law-Making // Legal Forum. 2015. No. 4.
- Ma Qiufeng. The Concept of Computer Crime // China Academic Journal Electronic Publishing House. 1992.
- Qianyun Wang. A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe. Rotterdam, 2016.
- Yu Zhigang. The Criminalization of Training Hackers in Cyberspace // Law Edition Journal of Yunnan University. 2015. No. 1.
- Zhao Bingzhi, Yu Zhigang. Computer Crime and the Response from Legislation and Legal Theory // China Legal Science. 2001. No. 1.
- Гудошников Л. М. Исследование политико-юридических проблем Китая в ИДВ РАН // Проблемы Дальнего Востока. 2005. № 6.
- Курс российского уголовного права. Общая часть / под ред. В. Н. Кудрявцева, А. В. Наумова. М., 2001.
- Лузянин С. Г., Трощинский П. В., Суходолов Я. А. Особенности правового регулирования борьбы с преступностью в Китае // Всероссийский криминологический журнал. 2016. Т. 10. № 4.
- Севальнев В. В. Правовое регулирование противодействия коррупции в Китае // Журнал зарубежного законодательства и сравнительного правоведения. 2018. № 2.
- Трощинский П. В. К вопросу о традиционных взглядах на право в китайском обществе // Вестник Университета им. О. Е. Кутафина. 2016. № 3.
- Трощинский П. В. Право Китая в зеркале российской науки // Государство и право. 2018. № 1.
- Чупрова А. Ю. Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции: дис. ... д-ра юрид. наук. М., 2015.