DOI: 10.25586/RNU.V9276.18.04.P.121 УДК 343.3/.7

Е.А. Русскевич

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ: СРАВНИТЕЛЬНО-ПРАВОВОЕ ИССЛЕДОВАНИЕ

Процесс проникновения кибернетических методов, а также инструментария информационно-коммуникационных технологий в механизм преступления (информатизация преступности) актуализирует необходимость научного осмысления подходов к определению уголовной ответственности за компьютерные преступления по зарубежному уголовному законодательству.

Статья предназначена для студентов, аспирантов, преподавателей, сотрудников правоохранительных органов, практикующих юристов, а также для всех, кто интересуется проблемами соответствующей тематики.

Ключевые слова*: *уголовное право, компьютерные преступления, информационно-коммуникационные технологии, информационная безопасность.

E.A. Russkevich

CRIMINAL RESPONSIBILITY FOR CRIMES COMMITTED USING INFORMATION AND COMMUNICATION TECHNOLOGIES: THE COMPARATIVE LEGAL STUDY

The process of penetration of cybernetic methods, as well as the tools of information and communication technologies into the mechanism of crime (informatization of crime), actualizes the need for scientific understanding of approaches to determining criminal liability for computer crimes under the foreign criminal law.

The article is intended for students, post-graduate students, teachers, law enforcement officers, practicing lawyers, as well as for all those who are interested in the relevant topics.

Keywords*: *criminal law, computer crimes, information and communication technologies, information security.

Трансграничность компьютерной преступности заставляет совершенно по-другому взглянуть на роль и значение сравнительного правоведения в решении конкретных отраслевых проблем отечественного уголовного права. Познание опыта зарубежных стран позволяет обогатить отечественную науку, критически осмыслить национальное законодательство, выявить его слабые и сильные стороны. Однако не менее важным является и то, что отчётливое понимание особенностей установления и реализации ответственности за компьютерные преступления является непременным условием эффективного взаимодействия с правоохранительными органами и правовыми системами других государств.

Значительный материал по заявленной теме, конечно же, содержит уголовное законодательство США, которые, пожалуй, одними из первых обратили

внимание на проблему действенного противодействия преступлениям, совершаемым с использованием компьютерных технологий. Ответственность за неправомерный доступ к компьютеру, компьютерной системе или компьютерной информации, которые могут быть отнесены к так называемой критической информационной инфраструктуре, предусмотрена §1030 Свода законов США [1]. Данное преступление относится к категории так называемых федеральных преступлений. На уровне сводов законов отдельных штатов выделяются главы о киберпреступлениях (глава 16 Свода законов штата Южная Каролина, глава 815 Свода законов штата Флорида, глава 41 Свода законов штата Арканзас и др.), в рамках которых преступлениями преимущественно признаются неправомерный доступ к компьютерной информации, неправомерная модификация компьютерной информации, создание и распространение в любой форме компьютерной информации, которая заведомо предназначена для совершения преступлений, неправомерное распространение информации о сетевых идентификаторах. В ряду традиционных уголовно-правовых запретов, пожалуй, можно выделить специфический состав преступления, предусмотренный ст. 5-41-204 Свода законов штата Арканзас об ответственности за незаконное использование шифрования (unlawful use of encryption) [2].

Следует отметить, что в отдельных штатах законодатель уделил особое внимание регламентации обстоятельств, которые могут выступать в качестве должной защиты (an affirmative defense) от уголовного преследования за совершение деяния, посягающего на безопасность компьютерных данных. Так, например, Свод законов штата Нью-Хемпшир в ст. 638.17 специально оговаривает, что лицо не может подлежать уголовной ответственности в случаях, если:

1) лицо было добросовестно убеждено, что правообладатель компьютера или компьютерной информации уполномочил его или должен был уполномочить на доступ к ним;

2) лицо не знало, не должно было и не могло знать, что доступ был осуществлён вопреки воли правообладателя компьютера или компьютерной информации [3].

Закон о неправомерном использовании компьютерных технологий Великобритании (Computer misuse act 1990) в качестве компьютерных преступлений называет: неправомерный доступ к компьютерной информации (ст. 1), неправомерный доступ в целях совершения иных преступлений (ст. 2), неправомерные действия в отношении компьютерных данных или нарушение правил эксплуатации средств хранения или обработки компьютерной информации (ст. 3), неправомерные действия в отношении компьютерных данных или нарушение правил эксплуатации средств хранения или обработки компьютерной информации, которые повлекли угрозу наступления тяжких последствий (ст. 3ZA), создание, приобретение или распространение компьютерных программ или компьютерной информации для совершения преступлений, предусмотренных статьями 1, 3 или 3ZA (ст. 3A) [4].

Уголовный кодекс Германии отдельно не выделяет группу компьютерных преступлений. В разных главах предусмотрена ответственность за фишинг (ст. 202b), неправомерную модификацию информации (ст. 303a), компьютерный саботаж (ст. 303b), а также выведение из строя особо важных объектов инфраструктуры (ст. 305a) [5].

В Сингапуре ответственность за совершение компьютерных преступлений определяется Законом Сингапура о неправомерном использовании компьютерных технологий (Singapore Computer Misuse Act) и уголовным законодательством (Singapore Penal Code). Преимущественно заимствуя опыт Великобритании, Закон Сингапура о неправомерном использовании компьютерных технологий устанавливает ответственность за неправомерный доступ к компьютерной информации (ст. 3), неправомерный доступ к компьютерной информации с целью совершения другого преступле-

ния (ст. 4), неправомерную модификацию компьютерной информации (ст. 5), несанкционированный доступ к сетям или услугам связи (ст. 6), неправомерное воспрепятствование использованию компьютера (ст. 7), неправомерное предоставление паролей, кодов доступа или иных аналогичных данных (ст. 8) [6]. Следует отметить, что в соответствии со ст. 3 указанного закона лицо подлежит ответственности за так называемое чистое хакерство (mere hacking), то есть преступление считается оконченным с момента самого неправомерного доступа и не требует наступления каких-либо общественно опасных последствий.

Действующее уголовное законодательство Китая предусматривает ответственность за: неправомерный доступ к компьютерной информации, содержащейся в критической информационной инфраструктуре (ст. 285^1), незаконное изменение данных, хранящихся в компьютерной информационной системе, и незаконный контроль над компьютерной информационной системой (ст. 285^2), распространение компьютерной информации, программ или иных средств для совершения преступлений, предусмотренных статьями 285^1–285^2 (ст. 285^3), неправомерное вмешательство в функционирование компьютерной системы (ст. 286). Самостоятельно криминализовано бездействие провайдеров в случаях их уклонения от исполнения обязательных решений контролирующих органов по блокированию соответствующих интернет-ресурсов, удалению запрещённой компьютерной информации и т.д. (ст. 286а).

Кроме того, ст. 287 Уголовного кодекса Китая, не описывая признаков какого-либо компьютерного преступления, содержит общее указание о том, что использование информационно-коммуникационных технологий для совершения других преступлений (мошенничества, коммерческого шпионажа, государственной измены и др.) подлежит юридической оценке по конкретным статьям об ответственности за данные преступления [7].

Закон о киберпреступлениях Австралии (Cybercrime Act 2001) классифицирует все преступления, совершаемые с использованием информационно-коммуникационных технологий, на две группы: тяжкие компьютерные преступления (serious computer offences) и другие компьютерные преступления (other computer offences). К первой группе относятся: неправомерный доступ к компьютерной информации или компьютерной системе в целях совершения тяжкого преступления (ст. 477^1), неправомерная модификация компьютерной информации (ст. 477^2), неправомерное нарушение электронной связи (ст. 477^3). Нельзя не отметить строгости наказаний за данные преступления – от 5 лет до пожизненного лишения свободы. При этом, специфической особенностью санкции ст. 477^1 является то, что она построена по ссылочному принципу – вид и размер наказания определяется санкцией конкретного тяжкого преступления, которое намеревалось совершить лицо, используя информационно-коммуникационные технологии (a person who is guilty of an offence against this section is punishable, on conviction, by a penalty not exceeding the penalty applicable to the serious offence… serious offence means an offence that is punishable by imprisonment for life or a period of 5 or more years) [8]. К иным компьютерным преступлениям австралийский законодатель относит неправомерный доступ к защищённой компьютерной информации (ст. 478^1), неправомерную модификацию компьютерной информации (ст. 478^2), приобретение и хранение (ст. 478^3), а также создание или распространение компьютерной информации или программ с целью совершения киберпреступлений (ст. 478^4).

Уголовный кодекс Норвегии регламентирует ответственность за неправомерный доступ к компьютерной информации (ст. 145) [9]. В ст. 146 (б) самостоятельно выделен запрет на распространение сведений о сетевых идентификаторах (логинах и паролях). Кроме того, в статье 151 (б) регламентирована ответственность до 10 лет лишения свободы за

уничтожение, повреждение или блокирование компьютерной информации или информационно-коммуникационного оборудования, которые повлекли существенное нарушение деятельности органов государственной власти или общественного порядка. Особо следует отметить, что ни одна из Скандинавских стран не устанавливает ответственности за создание, использование и распространение вредоносных компьютерных программ.

По вполне понятным причинам при проведении сравнительного исследования наиболее пристальное внимание следует обратить на особенности регламентации ответственности за компьютерные преступления по законодательству стран СНГ. В настоящее время наиболее развёрнутую систему компьютерных преступлений содержит Уголовный кодекс Республики Молдова – всего 10 составов [10]. Следует отметить, что отличительной особенностью УК Молдовы является криминализация только такого противоправного воздействия на компьютерные данные или систему, которое повлекло причинение ущерба в крупном размере. Так, уголовно-правовая норма о неправомерном доступе содержит указание на двухуровневые последствия – уничтожение, повреждение, модификацию, блокирование или копирование информации, нарушение работы компьютеров, информационной системы или сети и причинение ущерба в крупном размере. Равным образом уголовная ответственность наступает не просто за преднамеренное изменение, удаление или повреждение информационных данных, производство, импорт, продажу пароля, кода доступа или иных аналогичных данных, с помощью которых может быть получен доступ к информационной системе в целом или ее части, а только при условии, что эти действия повлекли причинение крупного ущерба.

Уголовный кодекс Республики Казахстан содержит девять составов преступлений, посягающих на отношения в сфере информатизации и связи (глава 7). Значимой особенностью уголовного законодательства Казахстана является то, что необходимым последствием неправомерного доступа к охраняемой законом информации, её уничтожения или модификации, а также неправомерного завладения выступают общественно опасные последствия в виде существенного нарушения прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства [11].

Похожую модель системы преступлений, связанных с использованием информационно-коммуникационных технологий, реализует УК Республики Туркменистан [12].

Практически идентичные списки уголовно-правовых запретов содержат УК Армении [13], УК Республики Беларусь [14] и УК Таджикистана [15]. При этом следует отметить удачное определение законодателем Таджикистана ответственности за нарушение правил эксплуатации компьютерной системы или сети. В диспозиции статьи содержится прямое указание на форму вины данного преступления – «…если это повлекло по неосторожности уничтожение, блокирование, модификацию компьютерной информации, нарушение работы компьютерного оборудования или причинение иного значительного ущерба». При этом деяния, связанные с умышленным посягательством на целостность и (или) доступность компьютерных данных, должны квалифицироваться либо как модификация компьютерной информации, либо как компьютерный саботаж.

Уголовный кодекс Республики Узбекистан насчитывает шесть составов преступлений, посягающих на отношения в сфере обеспечения безопасности информационных технологий (глава XX[1]) [16]. Законодатель Республики Узбекистан использует идентичный подход, реализованный в ст. 272 УК РФ, – в качестве обязательных последствий неправомерного доступа к компьютерной информации названы уничтожение, блокирование, модификация, копирование либо перехват информации. Вместе с тем, диспозиция ст. 278[2] УК РУ не содержит указания на то, что компьютерная информация, к

которой осуществляется неправомерный доступ, должна быть охраняемой законом.

Уголовное законодательство Украины выделяет шесть преступлений в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей, сетей электросвязи (раздел XVI) [17]. Достоинством украинского законодательства, на наш взгляд, является довольно успешное определение в ст. 362 субъекта преступления. Как известно, в науке уголовного права схожая проблема применительно к ст. 274 УК РФ до настоящего времени выступает предметом бескомпромиссной дискуссии. Кроме того, удачной представляется криминализация в ст. 363^1 так называемых DDOS-атак.

Уголовное законодательство Азербайджана в главе 30 «Киберпреступления» содержит пять составов [18]. В ряду квалифицирующих признаков совершения компьютерных преступлений УК Азербайджана содержится указание на «инфраструктурные объекты общественного значения». В соответствии с примечанием к ст. 271 УК Азербайджана, под такими объектами подразумеваются государственные учреждения, предприятия, организации, неправительственные организации (общественные объединения и фонды), кредитные организации, страховые компании, инвестиционные фонды, которые представляют большую значимость для государства и общества.

К особенностям законодательства Грузии, пожалуй, можно отнести установление ответственности юридических лиц в случае их причастности к киберпреступлениям. Возможными наказаниями выступают: штраф и лишение права заниматься определённой деятельностью или ликвидация и штраф [19].

Пожалуй, наименее проработанным в части обеспечения информационной безопасности является Уголовный кодекс Кыргызской Республики, который в настоящее время содержит лишь уголовно-правовой запрет на создание, использование и распространение вредоносных программ для ЭВМ (ст. 290). Следует, однако, отметить, что в проекте нового Уголовного кодекса Кыргызстана (вступает в силу с 1 января 2019 года) регламентированы уже три преступления против информационной безопасности (глава 42): неправомерный доступ к компьютерной информации (ст. 304), создание вредоносных компьютерных программ (ст. 305) и компьютерный саботаж (ст. 306) [20].

Подводя итог рассмотрению норм уголовного законодательства зарубежных стран, можно сделать вывод, что отечественное законодательство об ответственности за компьютерные преступления остро нуждается в коррекции. Не будет преувеличением утверждение, что УК РФ в действующей редакции не отвечает актуальным вызовам и угрозам в части обеспечения безопасности компьютерных данных и компьютерных систем. К числу первоочередных мер, на мой взгляд, следует отнести криминализацию компьютерного саботажа и неправомерного изменения идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создания, использования, распространения программ для изменения идентификационного кода абонентского устройства.

Литература

1. Электронный ресурс. – URL: https://www.law.cornell.edu/uscode/text/18 (дата обращения: 07.09.2017 г.).

2. Электронный ресурс. – URL: http://law.justia.com/codes/arkansas/2010 /title-5/subtitle-4/chapter-41/subchapter-2/5-41-206 (дата обращения: 15.09.2017 г.).

3. Электронный ресурс. – URL: http://law.justia.com/codes/new-hampshire/2015/title-lxii/chapter-638 (дата обращения: 07.09.2017 г.).

4. Электронный ресурс. – URL: URL: http://www.legislation.gov.uk/ukpga/ 1990/18/ section/2 (дата обращения: 15.09.2017 г.).
5. Электронный ресурс. – URL: https://www.gesetze-im-internet.de /englisch_stgb/ englisch_stgb.html (дата обращения: 08.09.2017 г.).
6. Электронный ресурс. – URL: http://statutes.agc.gov.sg (дата обращения: 14.09.2017 г.).
7. Электронный ресурс. – URL: http://www.fmprc.gov.cn/ce/cgvienna/eng/ dbtyw/ jdwt/crimelaw/t209043.htm (дата обращения: 07.09.2017 г.).
8. Электронный ресурс. – URL: https://www.legislation.gov.au/Details/ C2004A00937 (дата обращения: 07.09.2017 г.).
9. Электронный ресурс. – URL: http://www.un.org/depts/los/LEGISLATION ANDTREATIES/PDFFILES/NORpenal_code.pdf (дата обращения: 07.09.2017 г.).
10. Электронный ресурс. – URL: http://online.zakon.kz/Document/?doc_ id=30394923#pos=2668;-85 (дата обращения: 19.09.2017 г.).
11. Электронный ресурс. – URL: http://online.zakon.kz/m/Document/?doc_ id=31575252#sub_id=2050000 (дата обращения: 07.09.2017 г.).
12. Электронный ресурс. – URL: http://online.zakon.kz/Document/?doc_id =31295286#pos=2801;-159 (дата обращения: 12.09.2017 г.).
13. Электронный ресурс. – URL: http://www.parliament.am/legislation.php ?ID=1349&sel=show&lang=rus#24 (дата обращения: 21.09.2017 г.).
14. Электронный ресурс. – URL: http://www.pravo.by/document/?guid= 3871&p0=Hk9900275 (дата обращения: 06.09.2017 г.).
15. Электронный ресурс. – URL: http://online.zakon.kz/Document/?doc_id= 30397325#pos=3041;-130 (дата обращения: 11.09.2017 г.).
16. Электронный ресурс. – URL: http://www.lex.uz/pages/getact.aspx? lact_ id=111457 (дата обращения: 14.09.2017 г.).
17. Электронный ресурс. – URL: http://online.zakon.kz/Document/?doc_id =30418109#pos=2981;-97 (дата обращения: 07.09.2017 г.).
18. Электронный ресурс. – URL: http://online.zakon.kz/m/Document/?doc _ id=30420353#sub_id=2710000 (дата обращения: 07.09.2017 г.).
19. Электронный ресурс. – URL: https://matsne.gov.ge/ka/document/ downl oad/16426/143/ru/pdf (дата обращения: 05.09.2017 г.).
20. Электронный ресурс. – URL: http://online.zakon.kz/Document/?doc_ id=30222833#pos=0;0 (дата обращения: 02.09.2017 г.).

References

1. Elektronnyy resurs. – URL: https://www.law.cornell.edu/uscode/text/18 (data obrashcheniya: 07.09.2017 g.).
2. Elektronnyy resurs. – URL: http://law.justia.com/codes/arkansas/2010 /title-5/subtitle-4/chapter-41/subchapter-2/5-41-206 (data obrashcheniya: 15.09.2017 g.).
3. Elektronnyy resurs. – URL: http://law.justia.com/codes/new-hampshire/2015/title-lxii/chapter-638 (data obrashcheniya: 07.09.2017 g.).
4. Elektronnyy resurs. – URL: URL: http://www.legislation.gov.uk/ukpga/ 1990/18/ section/2 (data obrashcheniya: 15.09.2017 g.).
5. Elektronnyy resurs. – URL: https://www.gesetze-im-internet.de /englisch_stgb/englisch_stgb.html (data obrashcheniya: 08.09.2017 g.).
6. Elektronnyy resurs. – URL: http://statutes.agc.gov.sg (data obrashcheniya: 14.09.2017 g.).
7. Elektronnyy resurs. – URL: http://www.fmprc.gov.cn/ce/cgvienna/eng/ dbtyw/jdwt/crimelaw/t209043.htm (data obrashcheniya: 07.09.2017 g.).
8. Elektronnyy resurs. – URL: https://www.legislation.gov.au/Details/ C2004A00937 (data obrashcheniya: 07.09.2017 g.).

9. Elektronnyy resurs. – URL: http://www.un.org/depts/los/LEGISLATION ANDTREATIES/PDFFILES/NORpenal_code.pdf (data obrashcheniya: 07.09.2017 g.).
10. Elektronnyy resurs. – URL: http://online.zakon.kz/Document/?doc_ id=30394923#pos=2668;-85 (data obrashcheniya: 19.09.2017 g.).
11. Elektronnyy resurs. – URL: http://online.zakon.kz/m/Document/?doc_ id=31575252#sub_id=2050000 (data obrashcheniya: 07.09.2017 g.).
12. Elektronnyy resurs. – URL: http://online.zakon.kz/Document/?doc_id =31295286#pos=2801;-159 (data obrashcheniya: 12.09.2017 g.).
13. Elektronnyy resurs. – URL: http://www.parliament.am/legislation.php ?ID=1349&sel=show&lang=rus#24 (data obrashcheniya: 21.09.2017 g.).
14. Elektronnyy resurs. – URL: http://www.pravo.by/document/?guid= 3871&p0=Hk9900275 (data obrashcheniya: 06.09.2017 g.).
15. Elektronnyy resurs. – URL: http://online.zakon.kz/Document/?doc_id= 30397325#pos=3041;-130 (data obrashcheniya: 11.09.2017 g.).
16. Elektronnyy resurs. – URL: http://www.lex.uz/pages/getact.aspx? lact_id=111457 (data obrashcheniya: 14.09.2017 g.).
17. Elektronnyy resurs. – URL: http://online.zakon.kz/Document/?doc_id =30418109#pos=2981;-97 (data obrashcheniya: 07.09.2017 g.).
18. Elektronnyy resurs. – URL: http://online.zakon.kz/m/Document/?doc _ id=30420353#sub_id=2710000 (data obrashcheniya: 07.09.2017 g.).
19. Elektronnyy resurs. – URL: https://matsne.gov.ge/ka/document/ downl oad/16426/143/ru/pdf (data obrashcheniya: 05.09.2017 g.).
20. Elektronnyy resurs. – URL: http://online.zakon.kz/Document/?doc_ id=30222833#pos=0;0 (data obrashcheniya: 02.09.2017 g.).