УДК 341:34.03:004.056.5

Сабикенов С.Н., *Алиханова Л.М.

Казахсткий национальный университет имени аль-Фараби,
Республика Казахстан, г. Алматы
*E-mail: alikhanova.laura@mail.ru

ПРАВОВОЙ АНАЛИЗ ЗАКОНОДАТЕЛЬСТВА ЗАРУБЕЖНЫХ ГОСУДАРСТВ В ОБЛАСТИ БОРЬБЫ С СОЗДАНИЕМ, ИСПОЛЬЗОВАНИЕМ И РАСПРОСТРАНЕНИЕМ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ

Введение

Создание, использование и распространение вредоносных компьютерных программ является одним из видов преступлений, которые породил процесс информатизации. Так как сфера высоких технологий не знает границ, в мире нет сейчас ни одного государства, которое не столкнулось с тяжелыми последствиями компьютерных преступлений. Первыми с этим явлением стали бороться именно государства дальнего зарубежья. Это обусловлено тем фактом, что в них развитие передовых технологий началось раньше и происходило быстрее, нежели на постсоветском пространстве. По этой причине для совершенствования национального законодательства Республики Казахстан необходимо рассмотреть и проанализировать правовые основы борьбы с созданием, использованием и распространением вредоносных компьютерных программ в зарубежных государствах, имеющих более значительный опыт в деле противодействия компьютерным преступлениям.

Подход Соединенного Королевства

До разработки законодательства о компьютерных преступлениях суды Соединенного Королевства Великобритании и Северной Ирландии применяли акты гражданского права и Закон о преступном причинении ущерба имуществу 1971 года. Закон гласит, что лицо, которое намеренно без законного тому оправдания разрушает или наносит ущерб чужому имуществу, является виновным в преступлении [1]. В 1990 году был принят Закон о неправомерном использовании компьютерных технологий, который предусматривал три вида преступлений: несанкционированный доступ к компьютерной информации, несанкционированный доступ к компьютерным данным с намерением совершить или способствовать совершению дальнейших преступлений, несанкционированное изменение компьютерных данных. В данный законодательный акт были внесены изменения Законом о полиции и юстиции 2006 года, и формулировка названия раздела 3 была изменена на «несанкционированные действия, умышленно или по неосторожности препятствующие нормальной работе компьютера и т.п.». Вместе с тем Закон 2006 года увеличил максимальный срок лише-

ния свободы, предусмотренный разделом 3, до 10 лет [2]. И наконец, не менее существенным дополнением к Закону о неправомерном использовании компьютерных технологий 1990 года стало добавление раздела 4, который криминализировал изготовление, предоставление или приобретение предметов для использования в правонарушениях, связанных с неправомерным применением компьютерных технологий. Данный раздел содержит следующие основные положения:

1. Лицо виновно в совершении преступления, если оно изготавливает, приспосабливает, предоставляет или предлагает предоставить предмет в целях его использования для совершения преступления или чтобы способствовать совершению преступления, предусмотренного разделом 1 или 3.

2. Лицо виновно в совершении преступления, если оно предоставляет или предлагает предоставить предмет, осознавая, что этот предмет, вероятно, будет использован для совершения преступления или чтобы способствовать совершению преступления, предусмотренного разделом 1 или 3.

3. Лицо виновно в совершении преступления, если оно приобретает предмет в целях его дальнейшего предоставления для совершения преступления или чтобы способствовать совершению преступления, предусмотренного разделом 1 или 3.

4. В данном разделе «предмет» включает любую программу или данные в электронной форме.

Максимальный срок тюремного заключения за совершение преступления, предусмотренного разделом 4, составляет 2 года [2]. Данный Закон вызвал в Великобритании неоднозначную реакцию. Причина тому – распространение статьи не только на вредоносные программы, но и на программы, не являющиеся таковыми, но которые могут быть использованы в противозаконных целях [3].

Законодательство США

На федеральном уровне в Соединенных Штатах правовую основу борьбы с вредоносными компьютерными программами составляет принятый в 1986 году Закон о компьютерном мошенничестве и злоупотреблении, положения которого были включены в Титул 18 Свода законов США в виде §1030. Данный параграф гласит, что преступление совершает любой, кто сознательно осуществляет передачу программы, информации, кода или команды, и в качестве результата такого действия, намеренно причиняет несанкционированный ущерб защищенному компьютеру (§1030(a)5(A)). Наказанием за данное преступление в том случае, если оно повлекло нанесение ущерба, в общем составляющего как минимум 5000 долларов США в течение 1 года, одному или нескольким лицам, является штраф или 10 лет лишения свободы, или оба вида ответственности одновременно [4]. При этом под термином «защищенный компьютер» в данном параграфе понимается (1) компьютер, находящийся в исключительном пользовании финансового института или Правительства США, либо в случае, если он не находился в таком пользовании, компьютер, используемый правительством или финансовым институтом или в их интересах, а также (2) компьютер, который используется или задействован в междуштатной или межгосударственной коммерции или общении, включая компьютер, находящийся вне США, используемый таким образом, что он задействован в междуштатной или межгосударственной коммерции или общении США [4]. Как видно, в федеральном законодательстве речь идет об использовании вредоносной компьютерной программы, причем «поразить» такая программа должна именно «защищенный компьютер». Примечательно в данном случае использование законодателем формулировки «сознательно осуществляет передачу», так как вредоносные компьютерные программы зачастую обладают объективным свойством самораспространения и самоактивации, однако о применении вредоносной программы по небрежности или о неосторожном применении закон не упоминает. Ответственность за создание вредоносной компьютерной программы также не предусмотрена американским федеральным законодательством. Два последних факта создают риск того, что создатель вредоносной программы, написав ее код, запустит ее по неосторожности, тем самым ненамеренно причинив ущерб, но при этом избежав какой-либо ответственности.

Несколько иначе дело обстоит с законодательством на уровне штатов. Некоторые штаты, такие как Нью-Йорк и Нью-Джерси, применяют подход, близкий к подходу Закона о компьютерном мошенничестве и злоупотреблении. Законодательство этих штатов, равно как и федеральный закон, прямо не обращается к вредоносным компьютерным программам, а лишь затрагивает их постольку, поскольку они позволяют осуществлять несанкционированный доступ к компьютерной информации [5]. Однако в уголовном законодательстве штата Пенсильвания есть

положение, согласно которому лицо совершает преступление, если оно намеренно или сознательно продает, предоставляет или иным образом распространяет или хранит с намерением продать, предоставить или иным образом распространять компьютерное программное обеспечение или компьютерную программу, предназначенную или имеющую способность: (1) препятствовать, затруднять, контролировать, замедлять или нарушать нормальное функционирование компьютера, компьютерной программы, компьютерного программного обеспечения, компьютерной системы, компьютерной сети, компьютерной базы данных, сайтов всемирной компьютерной сети или телекоммуникационного устройства, или (2) ухудшать, блокировать, повреждать или разрушать деятельность компьютера, компьютерной программы, компьютерного программного обеспечения, компьютерной системы, компьютерной сети, компьютерной базы данных, сайтов всемирной компьютерной сети или телекоммуникационного устройства или любого сочетания вышеуказанного [6]. Законодательство Пенсильвании более конкретно говорит о вредоносных программах, при этом статья предусматривает как намерение программиста при разработке программы, так и свойства самой программы. Другими словами, если программа не имеет соответствующих вредоносных свойств, но разработана в противоправных целях, есть возможность привлечь виновное лицо к ответственности. Внимание следует обратить и на тот факт, что даже хранение вредоносной программы с противоправным намерением уже составляет оконченное преступление.

Бельгийский подход

В Королевстве Бельгия в 2002 году вступила в силу новая статья 550ter Уголовного кодекса. Статья криминализирует несколько видов деяний, основное деяние закреплено в §1 статьи, где закреплено, что любой, кто прямо или косвенно и с намерением нанести ущерб вносит, изменяет или удаляет данные в компьютерной системе или изменяет при помощи любого другого технологического устройства возможное применение данных в компьютерной системе, будет наказан лишением свободы от 6 месяцев до 3 лет и/или штрафом в размере от 26 евро до 25000 евро [7]. Здесь использован именно термин «данные», что говорит о попытке законодателя охватить широкий круг деяний, так как любая вредоносная компьютерная программа представляет собой данные, но этот термин не ограничивается только вредоносными программами. Для того чтобы привлечь к ответственности лицо, которое создало или распространило вредоносную программу, необходимо доказать, что деяние было совершено им с намерением нанести ущерб. Однако для того, чтобы привлечь к ответственности за совершение основного преступления также достаточно доказать преступное намерение, нет необходимости в том, чтобы ущерб был нанесен. Второй параграф статьи 550ter бельгийского Уголовного кодекса, однако, предусматривает, что, если компьютерная система фактически была повреждена в результате упомянутых выше действий, наказание может составить до 5 лет тюремного заключения, а размер штрафа может достигнуть 75000 евро. Кроме того, §3 Кодекса предусматривает ответственность лица, совершившего действия, описанные в первом параграфе, которые повлекли затруднение, полностью или частично, нормального функционирования компьютерной системы. Такое лицо наказывается лишением свободы сроком от 1 до 5 лет и штрафом в размере от 26 евро до 100 000 евро. Наконец, четвертый параграф гласит, что лицо, которое с мошенническим намерением или с намерением нанести ущерб создает, предоставляет, распространяет или сбывает данные, которые сохранены, обработаны или переданы, и это лицо осознавало, что они могут быть использованы для повреждения других данных или затруднить (полностью или частично) нормальное функционирование компьютерной системы, наказывается лишением свободы на срок от 6 месяцев до 3 лет и/или штрафом в размере от 26 евро до 100 000 евро [7].

Нидерландское законодательство

В Нидерландах вредоносные компьютерные программы являются специфическим видом манипуляции данными. Намеренное предоставление или распространение компьютерных вирусов криминализировано параграфом 3 статьи 350a Уголовного кодекса. Максимальное наказание за данное деяние составляет лишение свободы сроком на 4 года или штраф в размере 45 000 евро. Непреднамеренное (неосторожное) предоставление или распространение вирусов также уголовно-наказуемо согласно параграфу 2 статьи 350b, и максимальное наказание за него – 1 месяц тюремного заключения или штраф 2250 евро [8]. Вплоть до 2006 года под термином «вирус» понимались данные, предназначенные причинять ущерб путем самокопирования на компьютер. Учитывая, что только компьютерные черви причиняли вред таким способом, статья формально не распространялась на другие виды

вредоносных программ, однако было общепринято, что большинство вредоносных компьютерных программ также подпадало под действие данной статьи. Второй Закон о компьютерных преступлениях 2006 года изменил определение термина «вирус», подразумевая под этим словом данные, предназначенные для причинения ущерба [8].

Следует обратить внимание, что речь не идет о создании вирусов, а только лишь об их распространении и предоставлении.

Заключение

Проанализировав законодательные акты зарубежных государств, предусматривающие ответственность за создание, использование и распространение вредоносных компьютерных программ, можно сделать следующие выводы:

1. Подходы государств к борьбе с рассматриваемым видом преступления весьма разнообразны. Приведенные нами государства в данном вопросе можно разделить на две группы:

а) рассматривающие создание, использование и распространение вредоносных программ как более или менее самостоятельное преступление. Яркий пример тому – Соединенное Королевство Великобритании и Северной Ирландии. Хоть в данном случае программа и рассматривается только лишь как инструмент совершения других противоправных действий, существует оно автономно от них и представляет собой отдельный состав преступления;

б) рассматривающие создание, использование и распространение вредоносных программ как способ совершения иного преступления (главным образом манипуляции данными). Сторонник этого подхода – Соединенные Штаты Америки (в отношении федерального законодательства). Исключение составляют некоторые штаты, в числе которых приведенный выше штат Пенсильвания, который использует первый подход.

2. В большинстве рассмотренных нами государствах состав преступления создания, использования и распространения вредоносных компьютерных программ формальный, т.е. наступление последствий не является обязательным элементом состава преступления. Мы считаем такой подход наиболее приемлемым, так как вредоносные компьютерные программы способны нанести огромный ущерб, и с каждым днем они совершенствуются. Законодательство не должно ориентироваться только лишь на устранение последствий преступления.

3. В некоторых зарубежных государствах создание вредоносной компьютерной программы не относится к числу уголовно-наказуемых деяний (США). Ученые отмечают некоторые доводы, приводимые в пользу оставления создания таких программ ненаказуемым. В качестве одного из аргументов приводится наличие законной причины создавать вредоносные программы – для разработки и тестирования антивирусных программ. Действительно, создатели антивирусных программ часто сами пишут коды программ, которые обладают определенными вредоносными свойствами, и проверяют способность «антивирусов» противодействовать именно этим определенным свойствам вредоносных программ. Также противники криминализации создания вирусов приводят в качестве довода в свою пользу свободу выражения мнения, говоря, что написание вируса равносильно выражению своего мнения [5]. Оба аргумента не выдерживают критики. Против первого довода можно возразить следующее: вирусы, созданные в целях проверки антивирусных программ, создаются не с противозаконным намерением, и это можно было бы учесть при формулировке соответствующего состава преступления. Второй аргумент весьма сомнителен, так как существуют большие сомнения относительно того, можно ли рассматривать компьютерную программу как мнение или речь. Вновь исходя из вышеприведенного аргумента о необходимости ориентации законодательства на профилактику, считаем, что криминализация создания вредоносной компьютерной программы позволит предотвращать нанесение ущерба.

References

1 Klang M. A critical look at the regulation of computer viruses // International Journal of Law and Information technology. – 2003. – №2(11). – P. 162-183. URL: <http://www.digital-rights.net/wp-content/uploads/2008/01/klang_virus_ijlit.pdf>, Accessed: 11/02/2015

2 Computer Misuse Act 1990 // Official website of the United Kingdom's legislation. URL: <http://www.legislation.gov.uk/ukpga/1990/18/section/3A>, Accessed: 11/02/2015

3 Emm D. Cybercrime and the law: a review of UK computer crime legislation // Securelist.com: <https://securelist.com/analysis/36253/cybercrime-and-the-law-a-review-of-uk-computer-crime-legislation/>, Accessed: 11/02/2015

4 U.S. Code: Title 18 – Crimes and Criminal Procedure // Official website of the Cornell University Law School: <http://www.law.cornell.edu/uscode/text/18/1030>, Accessed: 12/02/2015

5 Kroczynski R.J. Are the Current Computer Crime Laws Sufficient or Should the Writing of Virus Code Be Prohibited? // Fordham Intellectual Property, Media and Entertainment Law Journal. – 2008. – № 18(3). – P. 817-865. URL: <http://law.fordham.edu/publications/article.ihtml?pubID=200&id=2738>, Accessed: 11/02/2015

6 Pennsylvania Consolidated Statutes. Act of Nov. 25, 1970, P.L. 707, No. 230 // Official website of Pennsylvania General Assembly: <http://www.legis.state.pa.us/cfdocs/legis/LI/consCheck.cfm?txtType=HTM&ttl=18&div=0&chpt=76&sctn=16&subsctn=0>, Accessed: 12/02/2015

7 Bruyndonckx B. Liability For The Creation And/or Distribution Of Viruses Under Belgian Law // Internet Business Law Services: <http://www.ibls.com/members/docview.aspx?doc=1585>, Accessed: 12/02/2015

8 Koops B.J. Cybercrime Legislation in the Netherlands. Country report for the 18th International Congress on Comparative Law, Washington, DC, 25-31 July 2010, session 'Internet Crimes' // Social Science Research Network: <http://ssrn.com/abstract=1633958>, Accessed: 12/02/2015