УДК 343.34

НЕКОТОРЫЕ ПРОБЛЕМЫ РОССИЙСКОГО ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

А.Н. Лямцев

ФГБОУ ВПО «Тамбовский государственный технический университет», г. Тамбов

Рецензент д-р юрид. наук, профессор В.Г. Баев

Ключевые слова и фразы: компьютерные преступления; проблемы российского законодательства; противодействие компьютерной преступности.

Аннотация: Рассмотрены вопросы противодействия компьютерной преступности. Исследовано законодательство в данной области. Проанализированы статьи главы 28 Уголовного кодекса Российской Федерации. Выявлено несоответствие наказаний совершенным деяниям в некоторых случаях, а также в целом несоответствие российского законодательства в данной сфере жестким мировым требованиям. Даны выводы по доработке законодательной базы в целях повышения эффективности борьбы с компьютерными преступлениями.

Использование компьютерных, информационно-коммуникационных технологий имеет бесспорные преимущества, однако, возможности быстро развивающихся технологий все чаще используются в преступных целях, о чем свидетельствует статистика компьютерных преступлений как в России, так и в зарубежных странах.

Цель данной работы – это выявление новых путей развития российского законодательства в сфере компьютерных преступлений, то есть поиск новых решений, которые помогут сократить количество данных правонарушений.

Актуальность этой проблемы является довольно значимой, так как в России совершается много компьютерных преступлений, и методы по борьбе с ними уже, в большинстве своем, исчерпали себя. Русскоязычные хакеры в 2011 году заняли второе место в мире по доходам, получив около 4,5 млрд долларов – это примерно треть рынка компьютерных преступлений. При этом преступники, живущие в самой России, заработали

Лямцев Александр Николаевич – аспирант кафедры «Уголовное право и прикладная информатика в юриспруденции», e-mail: alex-l.a.n@yandex.ru, ТамбГТУ, г. Тамбов.

2,3 млрд долларов, что на 1 млрд больше, чем в 2010 году [3]. По данным статистики, за первое полугодие 2012 года в России было зафиксировано 5696 киберпреступлений, что почти на 11 % больше, чем в аналогичном периоде 2011 года. Среди них преобладают преступления, связанные с созданием, распространением и использованием вредоносных программ, а также с мошенничеством в сети Интернет [1]. Данная статистика отражает лишь зарегистрированные преступления, тогда как на самом деле их может быть намного больше. Нужно искать новые пути развития, способные обеспечить более эффективную борьбу с компьютерными преступлениями и лицами, их совершающими.

В России на повестке дня стоит вопрос о создании новых органов и организаций, координирующих и осуществляющих борьбу с киберпреступностью, что, в свою очередь, требует подготовки национальных кадров, представителей, которых можно было бы привлекать на службу в транснациональные органы и организации, направленные на борьбу с киберпреступностью.

Основные виды преступлений, связанных с вмешательством в работу компьютеров:

1) несанкционированный доступ к информации, хранящейся в компьютере;

2) ввод в программное обеспечение «логических бомб», которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему;

3) разработка и распространение компьютерных вирусов;

4) преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, приводящая к тяжким последствиям;

5) подделка компьютерной информации;

6) хищение компьютерной информации.

В настоящее время все меры противодействия компьютерным преступлениям можно подразделить на технические, организационные и правовые.

К *техническим мерам* можно отнести: защиту от несанкционированного доступа к компьютерной системе, резервирование важных компьютерных систем; принятие конструкционных мер защиты от хищений и диверсий; обеспечение резервным электропитанием; разработку и реализацию специальных программных и аппаратных комплексов безопасности и многое другое.

К *организационным мерам* относятся: охрана компьютерных систем; подбор персонала; исключение случаев ведения особо важных работ только одним человеком; наличие плана восстановления работоспособности центра после выхода его из строя; организацию обслуживания вычислительного центра посторонней организацией или лицами, незаинтересованными в сокрытии фактов нарушения работы центра; универсальность средств защиты от всех пользователей; возложение ответственности на лиц, которые должны обеспечить безопасность центра; выбор места

расположения центра и т.п. Во всем мире и в нашей стране, в частности, техническим и организационным вопросам посвящено большое количество научных исследований и технических изысканий.

К *правовым мерам* следует отнести: разработку норм, устанавливающих ответственность за компьютерные преступления; защиту авторских прав программистов; совершенствование уголовного и гражданского законодательства, а также судопроизводства. К правовым мерам относятся также вопросы общественного контроля за разработчиками компьютерных систем и принятие соответствующих международных правил. Только в последние годы появились работы по проблемам правовой борьбы с компьютерной преступностью, и совсем недавно отечественное законодательство встало на путь борьбы с компьютерной преступностью. Поэтому представляется весьма важным расширить правовую и законодательную информированность специалистов и должностных лиц, заинтересованных в борьбе с компьютерными преступлениями.

На взгляд автора, с компьютерными преступлениями необходимо бороться, обеспечивая при этом свободу пользования и развития информационно-коммуникационных технологий, а также необходимо гарантировать свободу выражения мнений. Следует увеличить количество специальных подразделений по борьбе с компьютерными преступлениями. В данные подразделения могут быть привлечены люди, обладающие обширными познаниями в данной области. Множество молодых специалистов, в технической сфере или в правовой, могли бы оказать существенный вклад в борьбу с компьютерной преступностью. В некоторых случаях такие люди, не найдя применения своим знаниям в рамках закона, преступают его. Поэтому привлечение таких специалистов может стать одной из мер по борьбе с компьютерными преступлениями. Эти подразделения должны тесно сотрудничать с российской полицией и полицией других стран, чтобы укреплять международные усилия по борьбе с компьютерными преступлениями.

Кроме того, должны быть предусмотрены процедуры и системы, содействующие международному сотрудничеству. Например:

– возможность спонтанного получения и обмена информацией;

– возможность для властей одной страны собирать данные на территории другой страны, а также международная юридическая взаимопомощь;

– круглосуточная сеть, действующая без выходных, которой в любое время может воспользоваться расследование.

Необходимо повышать эффективность расследований компьютерных преступлений за счет:

– немедленного сохранения данных;

– предоставления властям возможности требовать получения конкретной информации;

– предоставления следствию возможности собирать данные о трафике и перехватывать контент в реальном времени.

Борьба с преступностью требует международного сотрудничества, и в особенности с преступностью компьютерной, ибо преступники действуют через границы и злоупотребляют различиями в национальных законодательствах.

Что касается международных документов, связанных с компьютерной преступностью, то основополагающим международным нормативным актом в сфере компьютерных технологий является Конвенция о компьютерных преступлениях СДСЕ № 185, открытая к подписанию в Будапеште 23.11.2001 [2]. Данная Конвенция стала первым в истории международным договором о преступлениях, совершаемых посредством сети Интернет и иных коммуникационных сетей. Она устанавливает принципы уголовной ответственности за нарушение авторского права, за мошенничество с использованием электронно-вычислительных машин, а также за нарушение безопасности компьютерных сетей. Приоритетная цель Конвенции состоит в определении общей политики в сфере уголовного права, направленной на защиту общества от компьютерных преступлений. На настоящий момент Конвенция ратифицирована 30 странами из числа членов Совета Европы, а также США. Российская Федерация несколько раз рассматривала вопрос о подписании Конвенции, но отрицательное решение, как следует из сообщений официальных информационных агентств, было принято из-за несогласия российских спецслужб предоставить иностранным правоохранительным органам возможность технического перехвата российского интернет-трафика.

Ратификация данной Конвенции могла бы привнести некоторые новшества в российское законодательство. В этом случае Российская Федерация будет обязана признать уголовно-наказуемыми действия по приобретению и владению для пользования устройств, включая компьютерные программы, разработанных или адаптированных для совершения какого-либо правонарушения (вредоносное программное обеспечение), а также компьютерных паролей, кодов доступа или иных аналогичных данных, с помощью которых может быть получен доступ к компьютерной системе в целом или любой ее части. Иными словами, российского интернет-пользователя ожидает тюремный срок уже за сам факт приобретения в целях использования так называемого «пиратского софта». При этом под приобретением программного обеспечения подразумевается, в том числе, его безвозмездное получение, например, «скачивание» с общедоступного интернет-ресурса. Нахождение подобного программного обеспечения на персональном компьютере пользователя будет также рассматриваться как совершение преступления. На настоящий момент уголовный закон России предполагает ответственность лишь за создание, использование и распространение вредоносного программного обеспечения. Законы в нашей стране по этому поводу довольно мягкие, и зачастую преступники получают лишь условный срок.

Последние изменения в Уголовном кодексе России затронули все три статьи главы 28: статью 272, 273, 274 УК РФ [4]. Так в статье 272 появился отдельный квалифицирующий признак – совершение неправомерного

доступа к компьютерной информации из корыстной заинтересованности. Но, однако, не обошлось без парадокса: максимальное наказание за неправомерный доступ из корыстной заинтересованности – шесть месяцев лишения свободы, а то же самое деяние, совершенное без подобной заинтересованности (например, из любопытства), наказывается двумя годами лишения свободы. Крупный ущерб, причиненный в результате неправомерного доступа, то есть составляющий сумму свыше одного миллиона рублей, также наказывается лишением свободы до шести месяцев. Деяние и наказание за него абсолютно не соизмеримы и данную ошибку необходимо устранить.

В судебной практике не обходится без курьезных случаев, которые показывают противоречивость применения законодательства на местах. Разные суды порой выносят диаметрально противоположные решения. Иногда это приводит к тому, что решение суда может противоречить Конституции РФ. Необходима выработка единой судебной практики, когда в похожих случаях решения будут соответствовать, а не различаться коренным образом. По некоторым вопросам, таким как использование torrent-клиентов для пирингового обмена данными через Интернет, судебной практики в РФ вообще не существует.

Таким образом, российское законодательство в настоящий момент не отвечает жестким «мировым требованиям» по борьбе с данным видом преступности. Необходимо устранение недочетов в законодательстве, наказания должны соответствовать совершенным деяниям. Недостаток судебной практики должен быть восполнен, основываясь на международном опыте. Многие страны, ратифицировавшие Конвенцию о компьютерных преступлениях СДСЕ № 185, гораздо успешнее ведут борьбу с компьютерными преступниками, так как имеют в своем распоряжении больше возможностей для этого. Ратификация Конвенции позволила бы повысить эффективность борьбы с компьютерной преступностью и в нашей стране. Конечно, только этого будет не достаточно, но серьезный шаг к затруднению деятельности преступников будет сделан и в дальнейшем законодательство не должно будет стоять на месте. Ему следует развиваться так же динамично, как развиваются новые технологии, и тогда к уже хорошо развитым техническим и организационным мерам защиты добавится полноценная правовая защита.

Список литературы

1. 30 сентября – День Интернета в России [Электронный ресурс] // Официальный сайт Министерства внутренних дел Российской Федерации. – Режим доступа : http://mvd.ru/news/item/146788/. – Загл. с экрана.

2. Конвенция о компьютерных преступлениях СДСЕ №: 185 от 23.11.2001 [Электронный ресурс] // Совет Европы. – Режим доступа : http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=1&CL=RUS. – Загл. с экрана.

3. Русскоязычные хакеры контролируют треть мирового рынка компьютерных преступлений [Электронный ресурс] // Технологии. – 2012. – 24 апр. – Режим доступа : http://hitech.newsru.com/article/24Apr2012/ruhack1in3. – Загл. с экрана.

4. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (с изм. и доп.) [Электронный ресурс] // Консультант-плюс. – Режим доступа : http://www.consultant.ru/popular/ukrf/. – Загл. с экрана.

Problems of the Russian Legislation in Computer Crimes

A.N. Lyamtsev

Tambov State Technical University, Tambov

Key words and phrases: combating computer crime; computer crime; problems of the Russian legislation.

Abstract: This paper considers the issues of combating computer crime; the legislation in this area has also been examined; Articles of Chapter 28 of the Criminal code of the Russian Federation have been analyzed; some discrepancy between penalties and committed acts in some cases has been revealed and, in general, the mismatch of the Russian legislation to the world's toughest requirements; the conclusions on the revision of the legislative framework to improve the efficiency of measures against computer crime have been made.
