

Интернет-преступления (киберпреступления) в российской уголовном законодательстве

Т.М. Хусяинов Т.М., г. Нижний Новгород

Глобальные процессы происходящие в политике, экономике, науке и технике оказали существенное влияние на все сферы жизни современного общества и отдельного человека в нём, привели к серьёзным изменениям или возникновению абсолютно новых феноменов.

Развитие и распространение новейших информационно-коммуникативных технологий (ИКТ) заметно меняет характер выполнения труда и структуру занятости населения, а также формы социально-трудовых отношений в современном обществе, причём это относится как к теневой стороне экономики, так и к переменам в криминальной занятости. В новой постиндустриальной экономике или информационной экономике, дистанционная занятость, а затем и Интернет-занятость получили широкое распространение именно благодаря развитию и распространению ИКТ, которые теперь выступают связующим звеном между наёмным работником (или фрилансером) и нанимателем. Подобная форма занятости успешно внедряется в целом ряде сфер трудовой деятельности, но особый интерес представляет криминальная интернет-занятость или интернет-преступность, так же известная как киберпреступность.

Под термином “Интернет-преступление” или “кибер-преступление” – стоит понимать весь спектр преступных действий в сфере информационных технологий, будь то преступления, которые совершены при помощи компьютеров, или те, предметом которых стали сами компьютеры, компьютерные сети и хранящаяся в них информация. “Компьютерное преступление” – это только то преступление, которое посягает на безопасное функционирование компьютеров и компьютерных сетей, а также на обрабатываемые ими данные. Таким образом, можно сделать вывод, что компьютерное преступление является разновидностью кибер-преступления [1, 2]. В тоже время Интернет-преступление включает в себя те противозаконные действия, которые были совершены по средствам сети Интернет.

В последние годы, в связи с бурным развитием и распространением информационных технологий и доступа к сети Интернет, их использованием практически во всех сферах жизни общества, проблема преступности в этой сфере приобрела особую остроту и актуальность. Данная проблема возникла в Западных странах уже во второй половине 1960 – начале 1970 годов, а в нашей стране – на рубеже 1970-1980-х годов. Первое преступление с использованием компьютера, совершенное на территории СССР, официально было зарегистрировано в 1979 г. в Вильнюсе (Литовская ССР). Факт данного преступления был зафиксирован в международный реестр правонарушений подобного рода и явился моментом возникновения и развития нового вида преступности в России. Основным средством борьбы с преступными

нарушениями нормального функционирования компьютерной техники должно было стать уголовное законодательство и совершение данного преступления поставило вопрос о необходимости поиска путей уголовно-правового регулирования ответственности этой категории правонарушений.

Первой попыткой ввести нормы борьбы с преступлениями в компьютерной сфере, стала разработка и представление 6 декабря 1991 г. проекта Закона РСФСР «Об ответственности за правонарушения при работе с информацией», в котором были предусмотрены основания для дисциплинарной, гражданско-правовой, административной и уголовной ответственности за подобные деяния, и предлагалось внесение поправок в Уголовный Кодекс РСФСР и другие Кодексы. Однако законопроект так и не был принят, что главным образом связано с общей неразработанностью законодательного поля в России в данной области права [3].

Следующая более успешная попытка в области реформирования уголовного законодательства явилось принятие Верховным Советом России постановления от 23.09.1992 № 3524-1 «О порядке введения в действие Закона Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных» [4]. Данный закон содержал положения о том, что выпуск под своим именем чужой программы для ЭВМ или базы данных либо незаконное воспроизведение или распространение таких продуктов влечет за собой уголовную ответственность. В пункте 5 Правительству РФ поручалось до 31.12.1992 подготовить и внести в установленном порядке на рассмотрение Верховного Совета РФ проекты законов о внесении изменений и дополнений в Гражданский и Уголовный кодексы, и другие законодательные акты, связанные с вопросами правовой охраны компьютерных программ и информации. Всего в 1992 г. было принято в общей сложности около 60 актов Верховного Совета России, Президента и Правительства в данной области, а в 1993 г. – уже более 100 [3].

В последующие годы власти по всему миру начинают уделять повышенное внимание к проблеме развития и распространения Интернет-преступлений, противодействию киберпреступности и вопросам упорядочения отношений в сфере информации.

Следующий этап развития российского уголовного законодательства в области компьютерной информации – разработка в 1994 г. проекта закона о внесении дополнений в Уголовный Кодекс РФ, которые установили ответственность за незаконное овладение программами для ЭВМ, файлами или базами данных; фальсификацию или уничтожение информации в автоматизированной системе; незаконное проникновение в автоматизированную информационную систему (АИС), совершенное путем незаконного завладения парольно-ключевой информацией, нарушения порядка доступа или обхода механизмов программной защиты информации с целью ее несанкционированного копирования, изменения или уничтожения; внесение и распространение «компьютерного вируса»; нарушение правил, обеспечивающих безопасность АИС. Но проект не был доведён до конца, в связи с постановкой новой задачи в виде формирования нового раздела о

преступлениях в области компьютерной информации, но уже в рамках нового Уголовного Кодекса РФ [3].

В январе-феврале 1995 г. был разработан и представлен проект нового Уголовного Кодекса РФ, в который уже была включена глава 29: «Компьютерные преступления». В данной главе определена ответственность за: самовольное проникновение в автоматизированную компьютерную систему (статья 271); неправомерное завладение программами для ЭВМ, файлами и базами данных (статья 272); самовольную модификацию, повреждение, уничтожение баз данных или программ для ЭВМ (статья 273); внесение или распространение вирусных программ для ЭВМ (статья 274); нарушение правил, обеспечивающих безопасность информационной системы (статья 275).

В дальнейшем специалистами в области IT и юристами были указаны существенные недоработки – отсутствие единой правовой концепции в данной главе, недостаточную связь с отраслевыми законами, слабую проработку терминологии, которая существенно отстала от времени, и стилистику. Дальнейшее развитие уголовного законодательства в области борьбы с киберпреступностью связано с принятием 20 февраля 1995 г. ФЗ Важное место в ряду нормативно-правовых актов в области компьютерного права занял Федеральный закон №24-ФЗ от 20 февраля 1995 г. «Об информации, информатизации и защите информации», в котором были даны определения для многих терминов данной сферы деятельности (информация, информатизация, пользователь (потребитель) информации и др.). Благодаря этому ФЗ и основным понятиям отражённым в нём правовое поле было лучше подготовлено для дальнейшего развития уголовного законодательства в этой сфере. По подсчётам некоторых исследователей [3] за период с 1992 г. по июль 1995 г. было принято около 500 нормативно-правовых актов по вопросам информационного законодательства, из которых 75 актов – полностью посвященным им, что также существенно повлияло на формирование информационного права и развитие уголовного права в сфере IT в России.

В 1996 г. был подписан Модельный уголовный кодекс государств-участников СНГ, в котором определена ответственность за компьютерные преступления.

1 января 1997 г. вступил в силу Уголовный кодекс РФ, содержащий главу 28 – «Преступления в сфере компьютерной информации», которая включает в себя 3 статьи:

- статья 272 «Неправомерный доступ к компьютерной информации»;
- статья 273 «Создание, использование и распространение вредоносных программ для ЭВМ»;
- статья 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети».

В 2011 году были внесены последние поправки [8] в главу 28 УК РФ, посвящённую регулированию борьбы с интернет-преступностью. Стоит отметить, что эти данные поправки не устранили все существующие

проблемы, как в законодательной, так и в правоприменительной деятельности, в связи с чем они по-прежнему сохраняют свою актуальность.

Отдельно отметим, что ответственность за преступления в Интернет-пространстве предусмотрена статьями 138.1, 146, 171.2, 183, 242, 242.1 Уголовного Кодекса РФ.

Следует обратить внимание на ряд существующих недоработок и проблем связанных с преступлениями в сфере компьютерной информации. Тарасенко М.Э. отмечает недостаток в определении “компьютерная информация” предлагаемом ст. 272 УК РФ. Законодатель определил форму, способы хранения и передачи, но не в достаточной степени определил само понятие «информация» [5, С. 14]. Кроме того в главе 28 УК РФ отсутствуют понятия «данные», «сообщение», «вредоносное программное обеспечение», что существенно затрудняет правоприменение данных статей.

Таким образом, рассматривая развитие уголовного законодательства России в области борьбы с преступлениями в Интернет-пространстве, мы можем отметить положительную динамику, развитие законодательства и высокий интерес со стороны законодателя. Проблема же “догоняющего” развития УК РФ, связано с тем, что развитие информационных технологий существенно опережает любое законодательное регулирование, т.к. требует немедленного правового реагирования, а общественная опасность данной категории преступлений существенно повышается в связи с проникновением их во все сферы жизни общества, государственные структуры и жизнь каждого отдельного человека.

можно отметить, что имеющаяся на данный момент ситуация (отсутствие или существенная ограниченность юридических моделей и определений для рассматриваемых общественно-опасных действий) требует немедленного правового реагирования, так как действующий Уголовный кодекс Российской Федерации (УК РФ) в полной мере не сможет решить все актуальные на сегодняшний день проблемы, связанные с преступлениями в информационной сфере. Кроме законодательного закрепления норм борьбы с киберпреступностью. Крайне необходимо разработать и повсеместно внедрить методы выявления, сбора доказательной базы и проведения оперативно-розыскных мероприятий в отношении Интернет-преступников, что требует серьёзных исследований, а в дальнейшем повышение квалификации сотрудников правоохранительной и судебной системы. Кроме того борьба с Интернет-преступностью требует серьёзных мер на международном уровне, в частности заключение договоров о взаимопомощи в правоохранительной деятельности в сфере компьютерной информации.

Для более эффективной борьбы с Интернет-преступностью необходимо устойчивое международное сотрудничество и разработка международно-правовых нормативных актов в данной сфере, т.к. сеть Интернет стала связующим звеном между людьми по всему миру, и позволяет информации преодолевать тысячи километров за считанные секунды. Интернет не обременен границами конкретных государств, поэтому борьба в отдельно взятой стране невозможна, а следовательно, необходимо закрепление норм

регулирующих и осуществляющих контроль информационной сферы на международном уровне.

Список литературы и источников

1. Тарасенко М.Э. Проблема борьбы с киберпреступлениями в Российской Федерации // Закон и общество: история, проблемы, перспективы: мат-лы межвуз. студ. науч. конф. Красноярск: Краснояр. гос. аграр. ун-т, 2013. С. 13-16.
2. Хусяинов Т.М. Криминальная Интернет-занятость (Интернет-преступность): определение и проблемы противодействия // Уголовный Закон Российской Федерации: проблемы правоприменения и перспективы совершенствования: материалы всероссийского круглого стола (25 апреля 2014). Выпуск 5 / главн.ред. П.А. Капустюк, отв.ред. Р.А. Забавко. Иркутск: ФГКОУ ВПО ВСИ МВД России. 2014. С. 230-236. DOI: 10.13140/RG.2.1.2313.9360
3. Маслакова Е.А. Правовое регулирование уголовной ответственности за преступления в сфере компьютерной информации в Российской Федерации // Правовые вопросы связи. 2006. №2. [Электронный ресурс]. Режим доступа: <http://www.center-bereg.ru/h1835.html>
4. Постановление ВС РФ от 23.09.1992 N 3524-1 «О порядке введения в действие Закона Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных» [Электронный ресурс]. – Справочно-правовая система «Консультант-Плюс».
5. Хусяинов Т.М. Основные причины распространения Интернет-преступности в молодёжной среде // Уголовное право в эволюционирующем обществе: проблемы и перспективы: сб. науч. ст. Ч. 1 / ред. кол.: С.Г. Емельянов [и др.]. Курск: Юго-Зап. гос. ун-т. 2014. С. 232-236. DOI: 10.13140/2.1.1827.6805
6. Волеводз А.Г. Российское законодательство об уголовной ответственности за преступления в сфере компьютерной информации // Российский судья. – 2002. – № 9. – С. 34–41. [Электронный ресурс]. Режим доступа: <http://mgimo.ru/files/114944/114944.pdf>
7. Филимонов С.А. Некоторые проблемы борьбы с киберпреступностью как самых опасных транснациональных преступлений // APRIORI. Серия: Гуманитарные науки. 2014. №1. [Электронный ресурс]. Режим доступа: <http://cyberleninka.ru/article/n/nekotorye-problemy-borby-s-kiberprestupnostyu-kak-samyh-opasnyh-transnatsionalnyh-prestupleniy>
8. Чекунов И.Г. Киберпреступность: понятие и классификация // Российский следователь. 2012. №2. [Электронный ресурс]. Режим доступа: <http://www.center-bereg.ru/h583.html>
9. Рассолов И.М. Киберпреступность: понятие, основные черты, формы проявления // Юридический мир. 2008. №2. [Электронный ресурс]. Режим доступа: <http://www.center-bereg.ru/h1529.html>
10. Филимонов С.А., Олейников А.А. Практические проблемы защиты прав потерпевших при привлечении к уголовной ответственности

киберпреступников // Современные проблемы науки и образования. 2014. №5. [Электронный ресурс]. Режим доступа: <http://www.science-education.ru/119-14541>

11. Жерновой М.В., Елисеева О.А. Место России в системе борьбы с транснациональной преступностью // Вестник ДВЮИ МВД России. 2014. №4 (29). С. 22-27.