ЕВДОКИМОВ К. Н.

ПРИЧИНЫ СТАНОВЛЕНИЯ И РАЗВИТИЯ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ В РОССИИ

Общественная опасность компьютерных преступлений во многом обусловлена возможностью использования высоких технологий для совершения умышленных преступлений различной степени тяжести и причинения материального ущерба в крупном и особо крупном размерах.

Эксперты ФБР провели анализ 2066 организаций и экстраполировали полученные результаты на всю страну. 1324 респондентов отметили, что в течение 12 прошедших месяцев терпели финансовые убытки от компьютерных преступлений. В среднем, одна компания теряла $24 тыс., а все респонденты потеряли $32 млн. По данным отчета, в 2005 г. примерно 2,8 млн организаций и компаний США сталкивались хотя бы с одним инцидентом нарушения компьютерной безопасности [1]. В 2006 г. британское Министерство торговли и промышленности опубликовало результаты опроса, посвященного проблемам информационной безопасности. Согласно опросу, размер ущерба от компьютерных преступлений теперь составляет 10 млрд фунтов стерлингов в год [2].

В России криминогенная ситуация в данной сфере также ухудшается из года в год. Так, по данным ГИАЦ при МВД России, еще в 2003 г. средний размер причиненного материального ущерба от одного нарушения авторских и смежных прав, совершенного с использованием компьютерных и телекоммуникационных технологий (квалификация преступного деяния по совокупности ст. 146 и 272 УК РФ), составлял 559,4 тыс. руб.; компьютерного мошенничества (ст. 159 и 272 УК РФ) – 423,9 тыс. руб.; изготовления или сбыта поддельных кредитных либо расчетных карт (машинных носителей информации) – 26,2 тыс. руб. [3].

По данным Следственного комитета при МВД России, ущерб только от компьютерного пиратства за первое полугодие 2009 г. составил более 600 млн руб. [4].

Кроме того, тенденция роста компьютерной преступности за последние годы остается довольно устойчивой и в связи с развитием современных технологий в банковской, торговой, управленческой и др. сферах, предпосылок для ее снижения в данный период времени не наблюдается. В чем же причина столь значительного роста преступлений в сфере компьютерной информации?

По мнению Ю. Гульбина, одной из основных причин возникновения компьютерной преступности вообще явилось информационно-технологическое перевооружение предприятий, учреждений и организаций, насыщение их компьютерной техникой, программным обеспечением, базами данных. Другой – реальная возможность получения значительной экономической выгоды за противоправные деяния с использованием ЭВМ. Появилась заманчивая возможность как бы обменивать продукт своего неправомерного труда на иные материальные ценности [5].

По нашему мнению, говоря о причинности компьютерных преступлений, совершаемых на территории России, следует выделить следующие значимые факторы:

• Мы можем говорить о социальных противоречиях между потребностями в программной (компьютерной) продукции и невозможностью (нежеланием) их удовлетворения легальными (законными) способами.

Переход России к рыночной экономике с гарантированной свободой предпринимательской деятельности обеспечил естественную конкуренцию между отечественными и зарубежными производителями программной продукции в области компьютерных технологий, тем самым на рынке должен присутствовать как бы отлаженный механизм регулирования спроса и предложения на такую продукцию. Однако на практике существует недобросовестная конкуренция в виде нарушения авторских и патентных прав производителя с целью получения недобросовестными конкурентами сверхприбылей от продажи так называемой «пиратской» продукции. При этом потребитель либо не в состоянии обнаружить подделку недоброкачественного товара, либо сознательно приобретает нелицензированную продукцию в силу ее дешевизны. Поэтому система саморегулирования рынка в данной ситуации не обеспечивает защиту законных правообладателей программного обеспечения и государство обязано вмешиваться в регулирование этих правоотношений [6].

• Это корыстные мотивы компьютерных преступников, преследующих цель получить какие-либо материальные или нематериальные блага.

Деятельность непосредственно самих «хакеров», «крекеров», «фримеров» и т. д., которые, имея необходимое компьютерное оборудование, с целью получения незаконной прибыли осущест-

вляют несанкционированное внедрение в компьютерные сети ЭВМ, в том числе через Интернет, и занимаются хищением компьютерной информации, представляющей коммерческий интерес.

При этом надо заметить, что так называемые «хакеры» в большинстве случаев работают по «найму», т. е. получают заказ на хищение нужной информации, либо привлекаются фирмами как специалисты для обнаружения несанкционированного доступа или утечки информации в корпоративных сетях ЭВМ.

• Это проблемы юридического (правового) характера в сфере борьбы с компьютерной преступностью.

В уголовном, гражданском и административном законодательстве окончательно не урегулирован вопрос оценки ущерба, причиненного компьютерными правонарушениями, критерии, которыми должен руководствоваться суд при определении размера этого ущерба и его возмещения виновными. Крайне несовершенной является и конструкция статей российского законодательства о привлечении к ответственности за компьютерные преступления и правонарушения (отсутствие многих квалифицирующих признаков, отягчающих наказание; упрощенная форма объекта посягательства и объективной стороны; небольшие санкции за совершенные деяния и мн. др.). Кроме того, по мнению автора, является пробелом отечественного уголовного законодательства отсутствие в ст. 272, 273 УК РФ санкции «лишение права занимать определенные должности или заниматься определенной деятельностью», что позволяет преступнику дальше совершать преступления. По нашему мнению, введение этого вида наказания носило бы ярко выраженный превентивный характер.

• Недостатки в деятельности дознания и предварительного следствия.

Большинство уголовных дел прекращаются на стадии предварительного следствия. Так, например, по данным ГИАЦ при МВД РФ, по реабилитирующим основаниям прекращены уголовные дела за неправомерный доступ к компьютерной информации: в 2004 г. – 134 [7], в 2005 г. – 372 [8], в 2006 г. – 267 [9].

В частности, из тридцати преступников, совершивших неправомерный доступ к компьютерной информации в Иркутской области в 2005 г., только в отношении семерых уголовные дела были направлены в суд, остальные уголовные дела прекращены по различным основаниям [10].

• Недостатки в деятельности органов и должностных лиц, осуществляющих оперативно-розыскную деятельность.

Здесь же мы можем сказать о недостатках в деятельности органов внутренних дел по раскрытию преступлений в сфере компьютерной информации. При многих УВД, ГУВД созданы отделы по борьбе с преступлениями в сфере высоких технологий (отделы «К» БСТМ при ГУВД, УВД РФ), которые практически на 100 % укомплектованы личным составом, но проблема высококвалифицированных кадров остается по-прежнему острой, так как подготовка сотрудников к выполнению поставленных задач остается недостаточной, что выражается в отсутствии специального образования и необходимой квалификации, в соответствии с последними достижениями в области компьютерных технологий. Кроме того, данные отделы по большей части укомплектованы сотрудниками, имеющими оперативный опыт по линии БЭП (борьбы с экономическими преступлениями), что связано с раскрытием преступлений в сфере нарушения авторских и смежных прав (ст. 146 УК) и изъятием контрафактной продукции. Однако они практически не имеют знаний и навыков по раскрытию преступлений в сфере компьютерных преступлений. Данную проблему можно было бы решить за счет привлечения выпускников кибернетических факультетов технических вузов, имеющих специальности «Информационная безопасность», «Информатика и информационно-компьютерные сети», «Системы автоматизированного проектирования» и др.

• Несовершенство судебной практики.

До сих пор отсутствуют разъяснения Пленума Верховного Суда по квалификации и определению наказаний за компьютерные преступления, что негативно сказывается на следственно-судебной практике и единообразии понимания и применения уголовно-правовых норм органами внутренних дел РФ. Кроме того, достаточно часто суды при рассмотрении дел о компьютерных преступлениях назначают наказание, не соответствующее общественной опасности деяния (штраф, условное осуждение с испытательным сроком), т. е. не связанное с лишением свободы.

• Это высокая латентность компьютерной преступности, ее скрытность, возникшая в связи с общей криминогенной обстановкой в стране, отсутствием и несовершенством имеющегося законодательства об ответственности за подобные деяния, а так-

же спецификой информационных отношений в сфере компьютерных технологий, требующих определенных навыков и познаний. При этом большая часть компьютерных преступлений так и остается незарегистрированной, так как многие сети ЭВМ не имеют защитного программного обеспечения или имеют упрощенные (устаревшие) степени защиты, что позволяет опытному «хакеру», совершив преступление, остаться незамеченным. При этом сотрудники служб безопасности фирм, корпораций имеющих сети ЭВМ, не имеют специализации и навыков в сфере компьютерной и информационной безопасности.

Начальник бюро специальных технических мероприятий МВД РФ генерал-полковник Борис Мирошников отмечает, что, «говоря о компьютерных преступлениях, мы часто повторяем, что в этой зоне наблюдается самая высокая латентность – до 80 %. Причина ее – нежелание жертв преступников по понятным причинам сообщать о постигших их неприятностях» [11].

По мнению независимых экспертов, только 10–15 % компьютерных преступлений становятся достоянием гласности, так как организации, пострадавшие вследствие совершения подобного рода преступлений, весьма неохотно предоставляют информацию, поскольку это может привести к потере их репутации или к совершению повторных преступлений [12].

• Организованный и профессиональный характер компьютерной преступности.

В наличии мы имеем все необходимые признаки [13] деятельности «хакеров» как профессиональных преступников:

1. Устойчивый вид преступного занятия (специализация).

«Хакеры» не совершают общеуголовных преступлений. Так, например, в Иркутской области из 134 лиц, в отношении которых были возбуждены уголовные дела по ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» в период с 2000 г. по 2005 г., ни один не имел судимости за общеуголовные преступления [14].

2. Получение преступного дохода (прибыли) в результате преступной деятельности.

3. Наличие у преступника необходимой квалификации (навыков пользователя ЭВМ или программиста) для совершения преступления.

4. Наличие у компьютерных преступников определенных правил, «законов» и терминологии [15], позволяющих им общаться, обмениваться опытом и находить единомышленников из числа пользователей ПЭВМ.

5. Наличие преступных связей с др. преступными элементами (как уже говорилось выше, многие «хакеры» работают по «найму»).

6. Наконец, мы с определенной долей уверенности можем говорить о разделении труда в компьютерной преступности, наличии соучастников (исполнителей, пособников, организаторов и др.) при совершении хищения информации в коммерческой или финансово-кредитной сферах.

• Высокая стоимость лицензионного программного обеспечения.

При этом пиратские копии не только дешевы или бесплатны, порой они даже лучше оригинальных. Так, Л. С. Симкин считает, что «Майкрософт и другие западные корпорации жалуются на многомиллионные убытки, понесенные по вине пиратов. Это, однако, не мешает им получать многомиллионные прибыли» [16]. Известный финансовый аналитик В. Гриднев сообщает, что «объем продаж программного обеспечения на европейском рынке в 2008 г. составил более 55 млрд евро, из 20 крупнейших компаний-поставщиков программного обеспечения на европейском рынке 75 % составляют американские компании» [17]. По нашему мнению, монополия на программный продукт является и средством экономического и политического контроля, формой поддержания зависимости «периферии» от «центра».

• Это доступность компьютерных технологий.

Как указывалось выше, «Информатика» как учебная дисциплина начинает изучаться школьниками с первого класса [18]. Каких-либо ограничений в приобретении компьютерной техники и программного обеспечения в нашей стране не существует. Россия занимает одно из первых мест в Европе по количеству компьютеров и пользователей сети Интернет. Поэтому несовершеннолетние, имеющие навыки программирования и пользования ЭВМ, находятся в состоянии постоянного «соблазна» применить свои знания на практике и получить ряд материальных, виртуальных или информационных благ незаконным путем.

• Это несерьезное отношение общества к компьютерной преступности в целом и компьютерным преступникам в частности.

Произошедшие на протяжении последних 15–20 лет политические события (развал СССР, образование РФ, переход к многопартийности и рыночной экономике, смена политического режима, дефолты и финансовые кризисы) привели к затянувшемуся экономическому и социальному кризису, отодвинув проблему компьютерной преступности в разряд второстепенных задач, что привело к ее неконтролируемому росту. В этой связи нельзя не поддержать А. В. Шопина, который еще в 1990-е гг. считал, что «отказ общественности от уголовного преследования компьютерных преступников ведет к отсутствию общего предупреждения, более того, он свидетельствует о "несерьезности" борьбы с компьютерными преступлениями и как бы приглашает других попробовать свои возможности» [19].

• Отсутствие надлежащего контроля со стороны государства за СМИ. Деятельность СМИ не только не активизирует борьбу общества с этим новым преступным проявлением, а иногда даже, наоборот, пытается оправдать преступников, выставляя их в свете «борцов за права», этаких современных «робин гудов». При этом некоторые печатные издания публикуют статьи, имеющие явно антиобщественный и криминальный характер, например: «Если тебе интересна тема взлома программ – пиши. И мы обязательно расскажем тебе о том, как взломать более сложные защиты и упакованные программы, как обойти антиотладочные приемы программистов и многое другое» [20]. В некоторых СМИ компьютерным преступникам приписывают необычную техническую одаренность, смелость, любознательность, предприимчивость и независимость духа. Достаточно вспомнить, с каким восторгом в некоторых изданиях живописались «подвиги» небезызвестных Митника и Левина [21]. Книги и журналы содержат каталоги «полезных» сайтов: www.XAKEP.ru, www.HACKZONE.RU, www.sdteam.com, www.oszone.net и др. [22]

Поэтому, по мнению автора, необходимо внедрять в массовое сознание граждан мысль о том, что компьютерная информация так же требует защиты, как и любая другая форма собственности, и что не вся компьютерная информация является общедоступной. Автором проводилось анкетирование 150 пользователей ЭВМ (студентов вузов г. Иркутска), и опрос показал, что 26,7 % не

знают об уголовной ответственности за неправомерный доступ к компьютерной информации, 40 % вообще не считают его преступлением, а 60 % не считают преступлением незаконное копирование компьютерной информации в личных целях.

Анализ вышеперечисленных причин возникновения и развития компьютерной преступности позволяет сделать вывод, что компьютерные преступления наносят большой материальный ущерб [23] физическим и юридическим лицам как в РФ, так и за рубежом, угрожают национальной безопасности России. Кроме того, в отличие от других незаконных источников доходов (торговля наркотиками, оружием и т. д.), компьютерная преступность является более безопасной и позволяет маневрировать большими (практически неограниченными) финансовыми ресурсами. Использование для преступных целей глобальной компьютерной сети Интернет позволяет преодолевать преступникам пограничные, таможенные, налоговые и иные границы государств, упрощая тем самым создание и функционирование преступных групп международно-регионального уровня. Все это говорит о том, что рост ущерба от компьютерных преступлений будет продолжаться, а компьютерная преступность становится средством получения крупных доходов организованной преступностью.

Примечания

1. URL: http://www.scr.ru\content.php?go=0&art=2&chapter=2865&do=0.

2. URL: http://www.xakep.ru\post\31307\default.asp.

3. См.: Вехов В. Б., Голубев В. А. Расследование компьютерных преступлений в странах СНГ : монография / под ред. Б. П. Смагоринского. Волгоград : ВА МВД России, 2004. С. 141.

4. URL: http://arhidelo.ru\press-center\rus\detail-14468.html

5 См.: Гульбин Ю. Преступления в сфере компьютерной информации // Рос. юстиция. 1997. № 10. С. 24.

6. См.: Федосов С. А. Уголовно-правовые и криминологические аспекты защиты авторских прав создателей и пользователей программ для ЭВМ и баз данных. М. : Моск. ин-т МВД РФ, 1999. С. 21.

7. См.: Приложение к письму ГИАЦ при МВД России № 34/4-160 от 03.05.05 г. «О направлении статистических данных».

8. См.: Ф. 1-ВТ (615) за 2005 г. Start2 & giz.mvd.ru [Электронный ресурс]

9. См.: Ф-1-ВТ (615) за 2006 г. Start2 & giz.mvd.ru

10. См.: Письмо ИЦ ГУВД Иркутской области РФ «О данных на лиц, привлеченных к уголовной ответственности по ст. 272 УК РФ в период с 2000 г. по 2005 г.» № 9/16-479 от 03.02.2006 г.

11. URL: http://www.zakon.kz\82167-v-rossii-v-2006-godu-vpervye-ostanovlen.html

12. См.: Карпов В. С. Уголовная ответственность за преступления в сфере компьютерной информации : дис. ... канд. юрид. наук. Красноярск : Краснояр. ГУ, 2002. С. 5.

13. См.: Криминология : учебник / под ред. В. Н. Кудрявцева и В. Е. Эминова. 2-е изд., перераб. и доп. М. : Юристъ, 2000. С. 613.

14. См.: Письмо ИЦ ГУВД Иркутской области РФ «О данных на лиц, привлеченных к уголовной ответственности по ст. 272 УК РФ в период с 2000 г. по 2005 г.» № 9/16–479 от 03.02.2006 г.

15. См.: Словарь жаргонных слов и выражений крэкеров, фрикеров, кардеров. Цит. по: Вехов В. Б., Голубев В. А. Расследование компьютерных преступлений в странах СНГ : монография / под ред. Б. П. Смагоринского. Волгоград : ВА МВД России, 2004. С. 256–272.

16. См.: Симкин Л. С. Программы для ЭВМ: правовая охрана (правовые средства против компьютерного пиратства). М. : Городец, 1998. С. 29–30.

17. URL: http://www.gridnev.info\?p=71

18. См.: Горячев А. В., Горина К. И., Суворова Н. И. Информатика в играх и задачах. Ч. 1 : учебник-тетрадь для 1-го класса : в 2 ч. М. : Баласс, 2005. 64 с.: ил.

19. См.: Шопин А. В. Компьютерные преступления: понятие и проблемы раскрытия // Компьютерные технологии в правоохранительной сфере. М., 1993. С. 52.

20. См.: Ильин С. Крэкинг – это просто // Хакер. 2005. № 8 (80). С. 75.

21. См.: Крылов В. В. Информационные компьютерные преступления. М., 1997. С. 63.

22. См.: Глушаков С. В., Бабенко М. И., Тесленко Н. С. Секреты хакера: защита и атака. М., 2008. С. 533.

23. См.: Вехов В. Б., Голубев В. А. Указ. соч. С. 6.

ЗЕЛЕНТ И. З.

ИТОГИ РАБОТЫ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ ИРКУТСКОЙ ОБЛАСТИ В ПЕРИОД ПЕРЕСТРОЙКИ И ПЕРЕХОДА К РЫНОЧНОЙ ЭКОНОМИКЕ

Вопрос, поставленный на обсуждение научно-теоретической конференции «Государственно-правовые проблемы развития России и Сибири: история и современность», чрезвычайно важен не только с исторической, но и с практической стороны. Знаменитые слова великого ученого М. В. Ломоносова: «Российское могущество прирастать будет Сибирью и Северным Океаном» стали пророческими и подтвердились реалиями современной России. Со времен Петра I изучение Востока России ставилось на научную основу. Большим достижением можно считать издание таких фундаментальных произведений, как «Атлас Всероссийской империи» И. К. Кириллова (1734) и «Атлас Российский» (1745), где впервые Сибирь и Дальний Восток были изображены с