Министерство образования и науки Российской Федерации
Федеральное агентство по образованию
Дальневосточный государственный университет

Р.И. Дремлюга

ИНТЕРНЕТ-ПРЕСТУПНОСТЬ

Монография

Владивосток
Издательство Дальневосточного университета
2008

ББК 32.973
Д73

Рецензенты
Н.В. Щедрин, доктор юридических наук, профессор;
А.А. Ширшов, кандидат юридических наук, доцент

Дремлюга, Р.И.
Д73 Интернет-преступность : моногр. / Р.И. Дремлюга. — Владивосток : Изд-во Дальневост. ун-та, 2008. — 240 с.
ISBN 978-5-7444-2114-4

Работа посвящена одной из актуальнейших и малоизученных проблем — Интернет-преступности. Охватывает ряд криминологических и уголовно-правовых проблем, связанных с распространением преступности в Интернет. Спам, террористическая деятельность в Интернет, субкультура хакеров — вот лишь неполный список вопросов, рассматриваемых в работе.

Рекомендована ученым в области уголовного права, криминологии; сотрудникам правоохранительных органов; специалистам, задействованным в борьбе с Интернет-преступностью; студентам юридических и технических вузов, а также широкому кругу читателей, интересующихся проблемами преступности в Интернет.

Д $\frac{2402040000}{180(03)\text{-}2008}$ ББК 32.973

ISBN 978-5-7444-2114-4

Оглавление

Введение

Стремительное внедрение цифровых технологий во все сферы человеческой жизни в конце XX — начале XXI вв. предопределило возникновение новых общественных отношений. Наибольшую значимость и распространенность имеет технология Интернет, которая соединила людей по всему земному шару, сделала коммуникации дешевыми и беспрепятственными и открыла новые горизонты для всего мирового сообщества. Интернет в последнее время дал человеку безграничные возможности в области передачи, распространения и рассылки информации, позволил выполнять финансово-банковские операции, несмотря на расстояния и границы. В России в 2007 г. по предварительным оценкам количество пользователей достигло 35 млн человек, то есть в этот процесс включен каждый четвертый россиянин[1]. В 2006 г. данная цифра составляла 22 млн, таким образом прирост составил порядка 40%[2] . Интернет стал не просто технологией, а уникальным новшеством, изменившим мир. Интернет — это место проведения досуга, возможность получать разнообразную информацию и свежие новости со всего мира, средство осуществления трудовой деятельности, способ найти единомышленника в самом удаленном уголке земного шара.

Представляется, что кроме положительного эффекта Интернет содержит ряд отрицательных моментов, приносит определенный вред и приводит к негативным последствиям. Некоторые особенности данной технологии, которые помогли ей распространиться по всему миру, в то же время создают благоприятные возможности для многих видов преступной деятельности. Новизна общественных отношений, возникших в результате появления Интернет, и отсутствие соответствующего правового поля, касающегося данной технологии, привели к множеству проблем, отрицательно влияющих на становление отношений в мировой компьютерной сети, основанных на законе.

---

[1]Количество Интернет-пользователей в России в 2007 г по предварительным оценкам выросло на 40 % до 35 млн человек [Электронный ресурс] / ПРАЙМ-ТАСС. — Режим доступа: http://www.prime-tass.ru/news/show.asp?id=756913&ct=news

[2] Каждый шестой россиянин является пользователем Интернета [Электронный ресурс] / Информационный портал Сибири. — Режим доступа: http://www.sibcity.ru/index.php?news=3545&line=people&page= 0&PHPSESSID=c

Вызывает опасение, что огромный технический потенциал и безграничные возможности Интернет все чаще в современных условиях могут быть использованы в преступных целях. При этом Интернет, с одной стороны, позволил более эффективно и безнаказанно совершать ранее существовавшие традиционные преступления, с другой — породил новые, неизвестные мировому сообществу еще совсем недавно виды общественно опасных посягательств. Глобальная сеть в последние годы стала использоваться не только для совершения общеуголовных преступлений, но и крайне опасных деяний международного значения — таких как «Сетевая-война», «Интернет-терроризм», «Интернет-забастовка», что создает угрозу безопасности целых государств и всего мирового сообщества.

Если еще несколько лет назад Интернет-преступления в России совершались редко, а Интернет-преступность как негативное социальное явление представляло реальную угрозу лишь в будущем, то в настоящее время следует констатировать, что доля сетевой преступности в структуре российского криминального мира существенно увеличилась.

Анализ статистических данных о преступности в сфере компьютерной информации показывает, что с 1997 по 2005 гг. в России количество зарегистрированных преступлений в сфере компьютерной информации (Глава 28 УК РФ) выросло более чем в 300 раз и достигло около 10000 преступлений за год. Хотя в последние годы наблюдается снижение регистрируемых преступлений (7236 — в 2007 г.), растет применение компьютерных технологий для совершения широкого круга преступлений (например, ст. ст. 146, 159, 242 УК РФ и т.д.). Интернет активно используется преступными элементами, широко распространены в сети сайты террористических организаций, рекламирующие и продающие наркотики и оружие, публикующие порнографические материалы, а также порталы расистской, националистской, экстремистской направленности и другие преступно ориентированные Интернет-ресурсы.

Высокая социальная опасность преступлений в Глобальной сети вытекает, прежде всего, из их транснационального характера, так как последствия подобных деяний могут охватывать неограниченный круг лиц в самых разных странах. При этом количество пользователей Интернет во всем мире в 2007 г. около полутора миллиарда и продолжает в наши дни стремительно увеличиваться, что предполагает дальнейший рост причиненного от Интернет-преступлений ущерба.

Необходимо отметить, что недостаток комплексных исследований, высокая латентность, как и отсутствие официальной статистки Интернет-преступности в России, приводят к неэффективности выработанных мер предупреждения, которые носят фрагментарный и противоречивый характер, предопределяя трудности в противодействии и борьбе с данным видом общественно опасных деяний.

Представляется, что в новых стремительно изменяющихся современных реалиях необходимы системное и последовательное исследование в России Интернет-преступности как в целом, так и отдельных наиболее распространенных ее видов, разработка эффективных мер борьбы и предупреждения преступлений в Глобальной сети, что будет способствовать развитию сетевых технологий в нашей стране.

Вопрос правовых отношений в Интернет, а также развитие законодательства в данной области осветили в своих работах С.А. Бабкин, Ю.М. Батурин, И.Л. Бачило, С.Д. Бражник, В.В. Воробьев,А.В. Геллер, А.М. Доронин, А.А. Жмыхов, А.М. Жодзишкий, Е.В. Красненкова, С.В. Молчанов, Д.С. Пушкин, Т.Г. Смирнова, Т.Л. Тропина, С.И. Ушаков, В.П. Числин, А.Е. Шарков, Д.А. Ястребов.

Криминологические исследования компьютерной преступности проводились такими российскими учеными, как М.С. Гаджиев, Д.В. Добровольский, Д.А. Зыков, Р.М. Кашапов, В.В. Колмыков, С.С. Наумов, Е.В. Старостина, Д.Б. Фролов.

Криминалистическая сторона данного вопроса проанализирована в работах В.Б. Вехова, М.М. Менжеги, Л.Н. Соловьева, Г.М. Шаповаловой, Н.Г. Шурухновой.

За рубежом проблему преступности в Интернет рассматривали в своих исследованиях В.А. Голубев, Б. Уорли (B. Worly), Д.Л. Шайндер (D.L. Shinder), Д. Чирилло (J. Chirillo), Т. Хардьено (T. Hardjono), Д. Шрейн и др. При этом следует отметить, что в работах зарубежных исследователей криминологическая и уголовно-правовая характеристика преступности в российском Интернет вообще не рассматривалась.

В настоящее время существует немало диссертационных работ, исследующих вопросы уголовной ответственности за компьютерные преступления и основные признаки компьютерной преступности: С.Д. Бражник, С.Ю. Бытко, В.В. Воробьев, М.С. Гаджиев, А.В. Геллер, Д.В. Добровольский, А.М. Доронин, К.Н. Евдо-

кимов, А.А. Жмыхов, Д.А. Зыков, Т.П. Кесареева, Е.В. Красненкова, Т.Г. Смирнова, М.В. Старичков, В.Г. Степанов-Егиянц, Т.Л. Тропина, С.И. Ушаков, В.П. Числин, А.Е. Шарков, Д.А Ястребов[3].

---

[3] Бражник С.Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: дис. ... канд. юрид. наук: 12.00.08. Ижевск, 2002; Бытко С.Ю. Некоторые проблемы уголовной ответственности за преступления, совершаемые с использованием компьютерных технологий: дис. ... канд. юрид. наук: 12.00.08. — Саратов, 2002; Воробьев В.В. Преступления в сфере компьютерной информации (юридическая характеристика и квалификация): дис. ... канд. юрид. наук: 12.00.08. — Нижний Новгород, 2000; Гаджиев М.С. Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан): дис. ... канд. юрид. наук: 12.00.08. — Махачкала, 2004; Геллер А.В. Уголовно-правовые и криминологические аспекты обеспечения защиты электронной информации и Интернета: дис. ... канд. юрид. наук: 12.00.08. — М., 2006; Добровольский Д.В. Актуальные проблемы борьбы с компьютерной преступностью: дис. ... канд. юрид. наук: 12.00.08. — М., 2005; Доронин А.М. Уголовная ответственность за неправомерный доступ к компьютерной информации: дис. ... канд. юрид. наук: 12.00.08. — М., 2003; Евдокимов К.Н. Уголовно-правовые и криминологические аспекты противодействия неправомерному доступу к компьютерной информации: дис. ... канд. юрид. наук: 12.00.08. — Иркутск, 2006; Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение: дис. ... канд. юрид. наук: 12.00.08. — М., 2003; Зыков Д.А. Виктимологические аспекты предупреждения компьютерного мошенничества: дис. ... канд. юрид. наук: 12.00.08. — Владимир, 2002; Кесареева Т.П. Криминологическая характеристика и предупреждение преступности в Российском сегменте сети Интернет: дис. ... канд. юрид. наук: 12.00.08. — М., 2002; Красненкова Е.В. Обеспечение информационной безопасности в Российской Федерации уголовно-правовыми средствами: дис. ... канд. юрид. наук: 12.00.08. — М., 2006; Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: дис. ... канд. юрид. наук: 12.00.08. — М., 1998; Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики: дис. ... канд. юрид. наук: 12.00.08. — Иркутск, 2006; Степанов-Егиянц В.Г. Преступления в сфере безопасности обращения компьютерной информации: сравнительный анализ: дис. ... канд. юрид. наук: 12.00.08. — М., 2005; Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук: 12.00.08. — Владивосток, 2005; Ушаков С.И. Преступления в сфере обращения компьютерной информации (теория, законодательство, практика): дис. ... канд. юрид. наук: 12.00.08. — Ростов-на-дону, 2000; Числин В.П. Уголовно-правовые меры защиты информации от неправомерного доступа: дис. ... канд. юрид. наук: 12.00.08. — М., 2004; Шарков А.Е. Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации: дис. ... канд. юрид. наук: 12.00.08. — Ставрополь, 2004; Ястребов Д.А. Неправомерный доступ к компьютерной информации: уголовно-правовые и криминологические аспекты: дис. ... канд. юрид. наук: 12.00.08. — М., 2005.

Как правило, в данных диссертационных исследованиях не подвергалась анализу криминологическая характеристика преступности в Интернет. Чаще всего авторы останавливались на изучении уголовно-правовых проблем преступлений, предусмотренных в Главе 28 УК РФ. Другие виды общественно опасных деяний, которые благодаря информационным технологиям вышли на новый качественный и количественный уровни, ими не затрагивались, а если в некоторых работах и давалась общая криминологическая характеристика компьютерной преступности, то она практически не отражала особенностей Интернет-преступности. Некоторые предложения авторов о выделении Интернет-преступности и Интернет-права в отдельную предметную область (Т.П. Кесареева, А.Л. Осипенко, И.М. Рассолов, А.А. Тедеев и другие), что необходимо для комплексной оценки параметров преступности в Глобальной сети, нуждаются в дальнейшем изучении и разработке.

Существующие работы освещали проблему лишь частично и не касались таких важных для Интернет-преступности вопросов, как особая криминальная субкультура сетевых преступников, детерминация современной Интернет-преступности; анализ характеристики личности преступника и потерпевшего; глубоко не исследовались и другие социально-значимые аспекты, связанные с Интернет-преступностью.

Представляется, что для выявления тенденций развития и для разработки мер предупреждения преступности в Глобальной сети следует более детально исследовать такое негативное социальное явление, как Интернет-преступность, а также проанализировать ее важные составляющие: личность преступника и личность потерпевшего, отношение разных слоев населения к проблеме Интернет-преступности; историю возникновения, тенденции развития уголовно-правового законодательства и криминологических мер предупреждения именно с учетом особенностей Интернет-технологии. Кроме того, вследствие быстрого роста количества Интернет-преступлений и усложнения структуры Интернет-преступности предпринята попытка проведения исследования текущего состояния и тенденций данного негативного явления с учетом стремительного видоизменения всех его характеристик.

В представленной монографии рассматривается Интернет-преступность как негативное социальное явление, влияющие на нее

процессы, а также характер воздействия на Интернет-преступность и возможные следствия подобного воздействия. На их фоне изучаются общественные отношения, складывающиеся по поводу совершения, пресечения, профилактики совершения преступных деяний посредством и с помощью Интернет. Исследованию подверглись криминологическая характеристика и основные детерминанты Интернет-преступности в РФ; система криминологических и уголовно-правовых мер по предупреждению, противодействию и борьбе с преступностью в глобальной сети Интернет.

Целью работы было выявление детерминирующих факторов и особенностей характеристики современной российской Интернет-преступности, криминологическая оценка ее основных показателей, разработка системы уголовно-правовых и криминологических мер профилактики и противодействия.

Согласно этой общей цели автором были поставлены следующие задачи:

— провести исторический анализ формирования и становления Интернет-преступности с момента зарождения до наших дней;

— проанализировать криминологические характеристики Интернет-преступности за последнее десятилетие в РФ;

— выявить характеристики личности Интернет-преступника в зависимости от вида совершаемого деяния;

— выявить виктимологические факторы, влияющие на совершение Интернет-преступлений ;

— провести анализ преступной субкультуры и ее роли в развитии и воспроизводстве Интернет-преступности;

— выявить общие и специфичные детерминанты Интернет-преступности в РФ;

— определить основные направления мер по борьбе с преступностью в Глобальной сети;

— разработать меры и рекомендации по предупреждению и борьбе с Интернет-преступностью в РФ.

Эмпирической базой научной работы стали статистические данные, полученные в ГИАЦ МВД России, ИЦ УВД Приморского края, материалы 137 уголовных дел Хабаровского и Приморского краев, Камчатской области по статьям Главы 28 УК РФ за 2002 — 2007 гг. Характеристика 144 лиц, выявленных в ходе следствия по данным уголовным делам легла в основу исследования личности преступника (всего в за эти годы в ДФО около 400 лиц). Для анали-

за личности потерпевших взяты 42 дела, содержавшие подробные сведения о жертвах Интернет-посягательств.

Также были проанкетированы разные группы населения (363 человека): 1) специалисты в компьютерных технологиях — компьютерные «Профессионалы» (127 чел.); 2) не имеющие образования в сфере информационных технологий, но пользующиеся Интернет, — «Гуманитарии» (149 чел.); 3) не умеющие и никогда не пользующиеся Интернет (87 чел.).

Было изучено в динамике последних лет более 2000 сайтов антисоциального и преступного содержания, в том числе для исследования доступности сведений и средств, облегчающих совершение преступлений в сфере компьютерной информации (1200 сайтов); «хакерской» субкультуры (257 сайтов); наркопреступности в Интернет (200 сайтов), террористической деятельности в Интернет (126 сайтов) и т.д.

Для поиска сайтов преступной направленности использовались популярные общедоступные российские поисковые системы: yandex.ru, google.ru, rambler.ru. Проанализированы материалы 114 уголовных дел по компьютерным преступлениям за рубежом, взятых с официального сайта департамента юстиций США, и других Интернет-ресурсов.

Проведено исследование 27 фильмов («Hackers», «Трон», «Сеть», «Взломщик» и др.); более 100 книг («Библия хакера», «Лабиринт отражения», «Дневник злобного хакера», «The art of deception», «The hacker's hadbook», «The hacker crackdown», «The Little Black Book of Computer Viruses» и другие); 24 песен («Про кардера Джекса», «О хакерах», «Вовка Хаккерр»), Интернет-сайты (257 — ресурсов); 14 периодических изданий («Хакер», «2600», «Phrack», «K-1ine» и т.д.) и других значимых для субкультуры хакеров источников на английском и русском языках. Также были проанализированы 1000 псевдонимов лиц на хакерских порталах.

В этой работе впервые определено понятие «Интернет-преступность» и данный вид преступности выделен в отдельную предметную область исследования; описаны уголовно-правовая и криминологическая характеристики основных показателей преступности в Глобальной сети.

Новым подходом является и то, что в отличие от других научных работ, преступность в Интернет и компьютерная преступность, их механизмы возникновения, функционирования и развития

объяснены в рамках теории субкультур. Определено понятие субкультуры Интернет-преступников, впервые системно проанализированы и описаны идеологическая база, обычаи, ритуалы, модели поведения, характерные для данной субкультуры, на основе не только научных трудов других авторов, но и работ самих хакеров как идеологического, художественного, публицистического, так и технического характера.

Впервые было проведено исследование общественного мнения об Интернет-преступности, анализ виктимологических аспектов, изучение и описание портрета личности современного Интернет-преступника; выделены особенности Интернет-преступности в России и выявлена система детерминирующих ее факторов; предложены методы борьбы с данным видом общественно опасных деяний. В порядке de lege ferenda предложены рекомендации по внесению изменений в УК РФ в соответствии с современными задачами противодействия Интернет-преступности.

В монографии есть ряд научных выводов и предположений, которые могут представлять научную ценность и также определяют научную новизну исследования. Вкратце их можно резюмировать следующими положениями:

• С момента возникновения Интернет-преступности в ходе ее эволюции автор выделяеи 5 последовательных этапов развития. Эти этапы, представленные в монографии, проходит Интернет-преступность в любой стране мира, меняются лишь быстрота прохождения того или иного этапа, но порядок остается тем же. В настоящее время, несмотря на отставание рассматриваемой категории российской преступности в прошлом, национальная преступность в Глобальной сети успешно интегрирована в международную Интернет-преступность и находится на четвертом этапе развития. Этап быстрого количественного роста совершаемых Интернет-преступлений совпал с ростом популярности субкультуры хакеров.

• Российская Интернет-преступность определяется как социально негативное явление, представленное в виде совокупности преступлений (запрещенных УК РФ деяний) и их системы, которые совершены посредством сети Интернет или с ее помощью с территории Российской Федерации; либо совершены с территории других государств, но направлены против интересов Российской Федерации. Интернет-преступность является частью компь-

ютерной преступности и смежна с такими ее видами, как преступность в сфере компьютерной информации, киберпреступность и т.д. Интернет-преступность отличается от других видов особыми свойствами: глобальность, широкая распространенность, крайне высокая латентность и др., определяющими бурный рост и общественную опасность. Отдельные Интернет-преступления обладают такими характеристиками, как неперсонофицированность; общедоступность; интеллектуальный и удаленный характер деяний, что отличает их от других видов деяний и т.д.

• Личность Интернет-преступника имеет свои специфические особенности, которые отличают ее от лиц, совершающих общеуголовные преступления традиционным путем. Интернет-преступники, по сравнению с исследованиями предыдущих лет, сильно «помолодели» и обладают большими профессиональными навыками.

• Для виктимологической профилактики исследуемого вида преступных деяний должны использоваться специфические компьютерные средства защиты, которые ранжируются в зависимости от ценности охраняемой компьютерной информации и навыков пользователя, а также средства защиты от «социальной инженерии». Автор приходит к выводу, что наиболее значимыми факторами виктимности исследуемых преступлений являются несоблюдение элементарных средств компьютерной безопасности и доверчивость пользователя, хотя причины меняются в зависимости от вида Интернет-преступления. На вероятность стать жертвой Интернет-преступления не влияют многие характеристики, свойственные большинству общеуголовных видов.

• Официальная статистика недостаточно точно отражает характеристику структуры, состояния и динамики современной российской Интернет-преступности. В связи с этим требуются дополнительные альтернативные источники информации, а также применение методик сбора и обработки данных для исследования преступности — как ее разновидностей, так и в целом. Из-за высокой латентности Интернет-преступности для установления истинных масштабов ее распространения требуется использование новых методов и источников получения информации, таких как контент-анализ сайтов, содержащих преступные сведения; анализ структуры сайтов с помощью поисковых систем, анализ числа посещений тех или иных сайтов, лингвистический анализ псевдонимов хакеров и т. д.

• Общество негативно относится к отсутствию контроля за деятельностью и распространением в Интернет информации социально-опасного характера. Большинство опрошенных в ходе проведенного нами исследования граждан одобряет введение уголовной ответственности за такие виды деятельности, как вербовка в националистические и террористические организации; распространение информации, позволяющей изготовить в домашних условиях взрывчатые вещества и взрывные устройства, а также за размещение в Глобальной сети информации по изготовлению в домашних условиях, приобретению и доставке наркотических средств и психотропных веществ. Одобрение обществом введения уголовной ответственности является одним из социальных условий криминализации, что подтверждает легитимность предлагаемых автором уголовно-правовых мер борьбы с Интернет-преступностью. В то же время отмечается, что некоторая часть населения склонна идеализировать образ Интернет-преступника, и часто воспринимает его как «борца за свободу».

• Преступная субкультура в Интернет определяется автором как совокупность идей, ценностей, обычаев, традиций, норм поведения, направленная на организацию образа жизни, целью которого является совершение Интернет-преступлений, их сокрытие и уклонение от правовой ответственности. Ценностный комплекс данной субкультуры служит также для легитимации и популяризации идеи хакерства в обществе.

• Сама природа сети Интернет является достаточно благоприятной для совершения преступлений. Такие свойства сети, как глобальность, трансграничность, анонимность пользователей, охват широкой аудитории, распределение основных узлов сети и их взаимозаменяемость создают преступникам, использующим Интернет, преимущества на всех этапах совершения преступления, а также позволяет эффективно скрываться от правоохранительных органов. Определяющими факторами, детерминирующими российскую Интернет-преступность, является специфическая криминальная субкультура, а также неразвитость сферы компьютерных технологий, что не всегда дает возможности легального заработка.

• Меры борьбы с Интернет-преступностью, которые существуют в настоящее время, не отвечают современным реалиям. Связано это не только с неэффективностью отдельных мер, но и с отсутствием целостной их системы, направленной на противодействие

Интернет-преступности. Наиболее эффективным в борьбе с Интернет-преступностью является комплекс криминологических мер профилактики, согласующихся с мерами социально-экономического, нравственно-идеологического, организационного, воспитательно-психологического и технического характера. Среди них выделяется одно из главных направлений — нейтрализация негативного влияния криминальной субкультуры компьютерных преступников.

• Действующий в настоящее время УК РФ не в полной мере соответствует современным требованиям борьбы с Интернет-преступностью и нуждается во внесении ряда изменений, отвечающих реалиям нашего времени, в общую и особенную части УК РФ. В монографии проведен анализ криминологических оснований изменения уголовного закона для совершенствования борьбы с компьютерной и Интернет-преступностью. Автор доказывает целесообразность и обосновывает ряд нововведений в УК РФ, таких как установление уголовной ответственности за нежелательную рассылку компьютерной информации (спам), введение в перечень отягчающих обстоятельств «совершение преступления посредством компьютерной сети» и др. В работе вы также можете найти предложения законодателю.

Значимость работы заключается в том, что данное монографическое исследование затрагивает уголовно-правовую и криминологическую проблемы, решение которых является необходимым условием для создания безопасного и прозрачного информационного пространства, а также напрямую связано с безопасностью многих сфер функционирования Российского государства. Именно от Интернет в современных реалиях зависит конкурентоспособность и безопасность большинства стран мира. Данная технология играет решающую роль в современной жизни, урегулирование вопросов правового контроля Интернет и установления надежного заслона для распространения Интернет-преступности является одной из основных проблем современного информационного общества.

Проведенное исследование восполняет недостаточную научную проработанность проблем, возникших в результате интенсивного роста количества и видоизменения качественных характеристик Интернет-преступлений, увеличения опасности деяний, с одной стороны, и отсутствия комплексных исследований в этой области — с другой.

Сформулированные теоретические выводы и положения могут быть полезны при разработке программ по борьбе с преступностью в Интернет в процессе осуществления системы мер государственной уголовной политики, совершенствования современного законодательства и правоприменения в области компьютерной и Интернет-преступности; а практические рекомендации могут быть использованы в области изучения отдельных Интернет-преступников и их группировок в оперативно-розыскной деятельности правоохранительных органов и во всесторонней профилактике данного вида преступлений. Кроме того, материалы исследования найдут применение при разработке и чтении лекции по курсам уголовного права, уголовно-исполнительного права, криминологии, криминалистики, юридической антропологии и психологии.

Глава 1. Понятие, уголовно-правовая характеристика и становление Интернет-преступности

1.1. История развития Интернет-преступности

В отличие от традиционных видов преступлений, история которых уходит в века, таких как убийство или кража, Интернет-преступность явление относительно молодое и новое. Нельзя говорить об Интернет-преступности в отрыве от сети Интернет. Именно такие свойства Глобальной сети, как быстрота и дешевизна трансакций, анонимность, трансграничность, создают уникальные условия для совершения новых видов преступлений и для качественного видоизменения традиционных. Так как Интернет-преступность неотделима от технологии, то начало отсчета следует вести с шестидесятых годов прошлого века, с момента создания сети Интернет. Именно появление и становление Интернет как глобальной сети представляется нам *первым этапом в развитии Интернет-преступности*. А всего, по нашему мнению, можно выделить 5 этапов в развитии преступности в Глобальной сети, каждый из которых отличается от предыдущего более сложной системой самой Интернет-преступности (единичные преступления; Интернет-преступность с несколькими чисто компьютерными специализациями; Интернет-преступность включающая в себя уже и традиционные виды преступлений; Интернет-преступность как международное явление).

История создания Интернет берет свое начало в 60-х годах. В 1962 г. доктор технических наук, профессор Джон Ликлайдер (J.C.R. Licklider), опубликовал свою концепцию широко распространенной компьютерной сети «Galactic Network» (Галактическая сеть). Он предполагал, что в будущем появится глобальная сеть, подключится к которой сможет любой желающий, и что данная сеть соединит компьютерные системы по всему миру. Его предположения подтвердились и сеть Интернет наглядное тому доказательство. Помимо общей идеи Ликлайдер подробно описал основополагающие принципы глобальной сети. Дж. Ликлайдер не мог предполагать, что данная сеть будет использоваться для осуществ-

ления платежей, передачи коммерческой информации и в других операциях, требующих высокой степени защиты от неправомерного доступа, с одной стороны, но с другой — широко распространенных.

В 1964 г. Леонард Клейнрок (сотрудник Массачусетского технологического института) доказал, что пакетный обмен данными — коммутация пакетов (передаваемая информация делится на части — пакеты и отправляется по разным каналам, чтобы в конце снова соединиться в одно целое) гораздо надежней циклического — коммутация каналов (данные передаются сплошным потоком по одному каналу). Пакетная технология была намного более удобной, обеспечивала высокую надежность передачи данных, позволяла сохранить работоспособность сети даже после остановки работы большинства ее узлов, именно этот принцип определяет свойства современной сети Интернет. При перекрытии одного канала передачи данных или при разрыве соединения во время работы пакеты начинают передаваться по другому каналу, что делает практически невозможным полностью перекрыть поток информации[4].

В 1965 г. с помощью телефонных линий соединили ЭВМ Массачусетского технологического с компьютером, находящимся в Беркли (Калифорния). Этим экспериментом было доказано, что для соединения компьютеров в сеть не обязательно проводить дополнительную коммуникационную сеть. Данный факт предопределил, что для передачи данных в последующем будут использоваться плохозащищенные от незаконного доступа телефонные линии.

Первым шагом к созданию Интернет стала коммуникационная сеть компьютеров ARPANet (Advanced Research Project Agency network, что в переводе означает «Сеть Управления перспективных исследовательских программ»), созданная по заказу Министерства обороны США. Идея данной разработки состояла в том, чтобы создать распределенную компьютерную систему без ярко выраженного центра, который можно было бы вывести из строя в случае ядерной войны, и состоящую из взаимозаменяемых сегментов. Уже тогда в сеть были заложены такие принципы, как распределенность и глобальность.

---

[4] Подтверждает это практика контроля за Интернет в Китае: несмотря на то, что выход в Интернет на многие сайты за пределами страны ограничен, хакеры из поднебесной легко находят обходные каналы.

В 1967 г. Лари Робертс, глава компьютерного отдела ARPA, опубликовал предварительную схему структуры сети ARPAnet. К этому времени уже были внедрены и опробованы необходимые технологии. В 1968 г. был представлен протокол обмена данными между компьютерами IMP's — родоначальник современного TCP/IP (самого распространенного протокола передачи данных в наши дни). Именно этому протоколу Интернет обязан многими своими свойствами, такими как неперсонофицированность, трансграничность и др. Протокол не был привязан к техническим средствам (в то время не было стандарта на компьютеры) и поэтому получил широкую распространенность, так что и широкая распространенность, и быстрое развитие сети во многом следствия удачной разработки данного протокола. В 1969 г. выпущен первый документ Request for Comment (RFC) под названием «Host Software» (Программное обеспечение узла сети).

В будущем все новые протоколы и разработки будут подробно описываться и рассылаться для того, чтобы избежать коллизий стандартов и протоколов. Схема принятия таких стандартов была достаточно прогрессивна. Сначала на конференциях обсуждались основные принципы и характеристики протокола. Затем группой специалистов разрабатывалась предварительная версия протокола, которая выносилась на всеобщее обсуждение. В отличие от принятия законов, когда законодатель может только предполагать его эффективность, компьютерные специалисты могли опробовать протокол на практике и протестировать характеристики.

Несмотря на этот факт, многие протоколы сети были созданы до того, как прообраз Интернет начал работать, что говорит о непродуманности многих моментов в архитектуре сети. В первую очередь это касается юридического контроля, который сильно затруднен при существующей структуре сети. Много внимания было уделено универсальности, распределенности, надежности, быстроте работы, но большинство вопросов безопасности и правового регулирования остались вне поля зрения, так как возникновение Интернет-преступности в то время никто не предвидел.

Расхождение теории с практикой дало о себе знать уже в ходе первых опытов с передачей компьютерных данных. В 1969 г. была осуществлена первая попытка передачи данных по новому пакетному протоколу. Первым узлом решили сделать компьютер, находящийся в Центре Сетевых Разработок в университете UCLA (University of

California Los Angeles — Калифорнийский университет в Лос-Анджелесе). Вторым узлом стал компьютер Стенфордского исследовательского института. Опыт закончился неудачей (сбой произошел в результате незначительной ошибки), но именно с него начинается история первой в мире компьютерной сети ARPAnet.

Сначала ARPANet состоял из четырех компьютеров, которые располагались в крупных исследовательских центрах[5]. Сеть планировалась для передачи информации и электронной переписки, поэтому никаких серьезных ограничивающих доступ элементов в ее структуре не присутствовало, так как появление компьютерных преступников тогда не предвидели. Это качество унаследует и сеть Интернет, что приведет к непредвиденному «анархизму» в сети[6]. Именно непродуманность вопросов безопасности и юридического контроля при разработке технических принципов сети, приведет к проблемам, с которыми мировое сообщество столкнется в будущем, что и является одной из причин широкого распространения противозаконной деятельности в Интернет.

В 70-х годах появляется термин «хакер», который позже станет применяться ко всем компьютерным преступникам, в том числе к Интернет-преступникам.

Представляется, что об Интернет-преступности становится известно с появлением первого профессионального преступника, занимающегося удаленными взломами телефонных коммуникаций, хотя было еще рано говорить об Интернет-преступности как широко распространенном явлении, но в большинстве литературных источников для хакеров и про хакеров именно Джон Дрэйпер (John Draper) упоминается как первый профессиональный Интернет-преступник (70-е годы). Он также породил первую специализацию хакеров — фрикеры (phreaker сокращенное от phone hacker — телефонный хакер). Именно поэтому, на наш взгляд, это время можно считать началом *второго этапа развития Интернет-преступности*, так как появилась первая специализация среди хакеров. В частности, Джон Дрэпер занимался взломом теле-

---

[5] Кесареева Т.П. Криминологическая характеристика и предупреждение преступности в Российском сегменте сети Интернет: дис. ... канд. юрид. наук: 12.00.08. — М., 2002. — С. 36.

[6] Касперски К. Техника отладки программ без исходных текстов. — СПб.: БХВ-Петербург, 2005. — С. 24.

фонных сетей, что позволяло осуществлять междугородние и международные звонки бесплатно. Он стал знаменит благодаря открытию того факта, что простой свисток издает сигнал с частотой 2600 Гц. Это была частота, необходимая для доступа к управляющим системам корпорации «AT&T» (монополист телефонной связи в Америке).

Джон Дрейпер разработал устройство, в состав которого входили свисток и телефонный аппарат. Данное приспособление позволяло делать бесплатные звонки, в том числе международные и междугородние. Он не стал скрывать свое ноу-хау и в журнале «Esquire» была издана его статья под названием «Секреты маленькой синей коробочки», в которой описывался алгоритм изготовления устройства для бесплатных звонков. Данный факт свидетельствует о зарождении субкультуры Интернет-преступности — первый официально зарегистрированный случай пропаганды в печати ее антиобщественных ценностей. Кроме того, была продемонстрирована незащищенность не только протоколов Интернет, но и телефонных линий, что обозначило еще одно слабое место будущей сети.

В рядах фрикеров в то время были даже такие знаменитые люди, как Стив Возняк (Steve Wozniak) и Стив Джобс (Steve Jobs), которые в будущем основали "Apple Computers" (всемирно известная корпорация, занимающаяся производством компьютеров); они наладили производство устройств для взлома телефонных сетей в домашних условиях. Сейчас в сфере интересов фрикеров ip-телефония сотовая и спутниковая связь.

В 1983 г. в США в штате Милуоки произошел первый арест Интернет-преступника, о котором известно общественности. Первый зарегистрированный Интернет-взлом был совершен группой из шести подростков, которая называла себя «группа 414» (414 — междугородний телефонный код Милуоки). В течение девяти дней ими было взломано 60 компьютеров, среди которых компьютеры Лос-Аламосской государственной лаборатории (место исследования ядерного оружия). Один из членов группы дал показания и остальные ее участники получили условный срок (probation) наказания на основании показаний первого[7].

---

[7] Лукацкий. А. Хакеры управляют реактором [Электронный ресурс] / Центр исследования компьютерной преступности. — Режим доступа: http://www.crime-research.org/library/Lukac0103.html

В восьмидесятых годах начинает наблюдаться количественный рост компьютерных атак. Центр исследования Интернет-безопасности CERT, открывшийся в 1988 г., фиксирует увеличение количества компьютерных атак, о которых сообщают пользователи Интернет. Если в 1988 г. было всего шесть обращений в центр, то в 1989 г. — 132, а в 1990 г. — уже 252. Интернет-преступность уже не редкость, появляются крупные хакерские группы, и Интернет начинает использоваться для более широкого круга преступлений. Это означает *начало третьего этапа в развитии Интернет-преступности*. На третьем этапе стремительно появляются новые специализации Интернет-преступников.

В 1984 г. Фред Коэн (Fred Cohen) опубликовал сведения о разработке первых вредоносных саморазмножающихся компьютерных программ и применил к ним термин «компьютерный вирус». Он написал программу, демонстрировавшую возможность заражения одного компьютера другим и предвосхитил возможность появления антивирусных программ. Первый свободно распространяющийся вирус для персональных компьютеров, называющийся «Brain» («Мозг») и заражающий только посредством дискет, появился в 1986 г. Он был создан в Пакистане двумя программистами с целью защиты от несанкционированного копирования их продуктов, но был воспринят как серьезная угроза среди американских пользователей. Первая антивирусная программа, которая могла предупредить распространение вредоносных программ, была опубликована через два года.

В 1986 г. в США принят первый компьютерный закон The Computer Fraud and Abuse Act[8], данный закон запрещал неавторизованный доступ к любой компьютерной системе и получение секретной военной информации[9]. В этом же году арестован член груп-

---

[8] См: http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001030———000-.html; http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act.

[9] Также данный закон защищал три вида несекретной информации. Во-первых, информацию, принадлежащую финансовым учреждениям (например, информация о кредитных картах и счетах), во-вторых, данные, принадлежащие правительственным учреждениям. В-третьих, информацию, принадлежащую международным или межштатовым организациям. Также закон содержал статьи, запрещающие повреждение данных (например, распространение вирусов).

пы Legion of Doom Лойд Бланкеншип (Loyd Blankenship), известный как The Mentor, во время отбывания наказания в тюрьме он пишет знаменитый «Манифест хакера» («Hacker's manifesto», иногда как «Conscience of a Hacker» — «Совесть хакера»). Идеи, высказанные в этом манифесте, считаются основой хакерской идеологии, они широко растиражированы в Интернет[10]. Заметим, что количественный скачок Интернет-преступлений совпал с ростом популярности в компьютерном мире хакерских идей, что свидетельствует о взаимосвязанности данных явлений.

В 1994 г. мир узнал о так называемом «деле Владимира Левина», отнесенном международной уголовной полицией к категории «транснациональных сетевых компьютерных преступлений». Это первое громкое дело с участием российских компьютерных преступников. Международная организованная преступная группа в составе 12 человек, используя Интернет и сеть передачи данных «Спринт/Теленет», преодолев защиту от несанкционированного доступа, попыталась осуществить 40 переводов денежных средств на общую сумму 10 млн 700 тыс. 952 доллара США со счетов клиентов названного банка, находящихся в 9 странах мира, на счета, расположенные в США, Финляндии, Израиле, Швейцарии, Германии, России, Нидерландах. Однако реально им удалось похитить только 400 тыс. долларов, после чего их преступная деятельность была пресечена[11]. Это была первая крупная международная финансовая махинация с использованием Интернет, которая стала известна широкой общественности. Интернет стал выходить на международную арену, а вместе с этим и Интернет-преступления становятся угрозой всему мировому сообществу.

Согласно сообщению Washington Post, в 1998 г. 12-летний хакер проник в компьютерную систему, которая контролировала водоспуск плотины Теодора Рузвельта в Аризоне. В случае открытия

---

[10] Если ввести в поисковой строке службы Yandex.ru словосочетание «манифест хакера», то поисковая служба выдаст не менее 1500 электронных ссылок. Отрывки данного манифеста цитируются в одном из самых популярных англоязычных фильмов о компьютерных преступниках «Хакеры» (The Hackers), вышедшем в 1995 г. в США.

[11] Кураков Л.П., Смирнов С.Н. Информация как объект правовой защиты. — М.: Гелиос, 1998. — С. 220—221; Владимир Левин (Биография) [Электронный ресурс] / ЛЮДИ. — Режим доступа: http://www.peoples.ru/state/criminal/computer/levin/

сливных ворот вода могла затопить города Темп («Tempe») и Месэ («Mesa») с общей численностью населения в 1 млн человек[12]. Это привело к появлению терминов Интернет-терроризм, компьютерный терроризм, кибертерроризм. Наиболее уязвимой к Интернет-атакам является сама Сеть, так как ее ключевые узлы доступны по Интернет из любой точки мира; кроме этого данные системы привлекают много хакерского внимания. Появление таких терминов, как Интернет-терроризм и громкие дела о преступной деятельности международных группировок, свидетельствуют о том, что в это время Интернет-преступность стала приобретать такое свойство, как транснациональность. Это свидетельствовало о начале *четвертого этапа в развитии Интернет-преступности*.

Серьезные последствия теперь могли наступать не только в случае умышленных Интернет-атак, но и по вине невнимательных компьютерных специалистов. Так, в 1997 г. ошибка сотрудника Network solutions привела к тому, что сайты, чьи имена заканчивались на «.net» и «.com» стали недоступными. Сбой в работе всей Глобальной сети произошел из-за невнимательности всего одного человека, этот факт свидетельствует о том, что направленные усилия нескольких человек (например, членов террористической организации) могут привести к еще более тяжким последствиям.

Буквально через четыре года, в октябре 2002 г. была совершена атака, целью которой была остановка работы всей инфраструктуры Глобальной сети. Более десяти основных DNS-серверов, от которых зависит работа всего Интернет, подверглись DoS-атаке (Dos сокр. от Denial of Service — атака на отказ работы), начавшейся одновременно с множества компьютеров по всему миру. Только нескольким удалось устоять. Большой уровень избыточности, присущий структуре сети, что связано с изначальным расчетом на устойчивость к ядерной войне, позволил избежать остановки коммуникаций, несмотря на выход из строя двух третей основных узлов.

Интернет-атаки со временем также стали способом достижения политических целей. Интернет-забастовка — это реализация забастовки в Глобальной сети. Участники такой акции одновре-

---

[12] Robert Lemos. Cyberterrorism: The real risk [Электронный ресурс] / Центр исследования компьютерной преступности. — Режим доступа: http://www.crime-research.org/library/Robert1.htm

менно заходят на сайт или подключаются к сервису, либо посылают электронные сообщения, пишут в форумах, для того чтобы ограничить либо вообще прекратить доступ на сайт другим пользователям. Происходит перегрузка Интернет-сайта или службы внешними запросами, что приводит к сбоям в работе или полной остановке.

Первый подобный протест осуществила группа, называющая себя «Strano Network», протестовавшая против политики французского правительства в вопросах ядерных программ и в социальной сфере. 21 декабря 1995 г. эта группа в течение часа атаковала различные сайты правительственных агентств. Участники группы с разных континентов были проинструктированы следующим образом: им полагалось с помощью браузера (программа просмотра Интернет-сайтов) одновременно зайти на правительственные сайты. Некоторые сайты действительно были выведены из строя на небольшое время[13].

В дальнейшем транснациональность проблемы Интернет-преступности проявляется все шире. Так, конфликт в Косово считается первой Интернет-войной. Компьютерные активисты использовали сеть Интернет для осуждения военных действий как Югославии, так и НАТО при помощи умышленного нарушения работы правительственных компьютеров и получения контроля над сайтами с последующим изменением содержимого, называемым «дефейсом» (англ. deface). В Интернет распространялись истории об опасностях и ужасах войны, а политики и общественные деятели использовали всемирную паутину для того, чтобы их призывы достигли как можно более широкой аудитории[14].

В настоящее время практически любой военный или политический конфликт сопровождается организованным противоборством в сети Интернет. Например, волна Интернет-атак в 2005 г.

---

[13] Д. Деннинг. Активность, хактивизм и кибертерроризм: Интернет как средство воздействия на внешнюю политику [Электронный ресурс] / Владивостокский центр исследования организованной преступности / Пер. Т.Л. Тропиной — Режим доступа: http://www.crime.vl.ru/index.php?p=1114&more=1&c=1&tb=1&pb=1

[14] А. Андреев, С. Давыдович. Об информационном противоборстве в ходе вооруженного конфликта в Косово [Электронный ресурс] / «ПСИ-ФАКТОР» Центр практической психологии. — Режим доступа: http://www.psyfactor.org/warkosovo.htm

спровоцирована школьным учебником истории, вышедшим в Японии, который искажает события в Китае в 1930 — 1940-х гг. XX века, в том числе умалчивает о военных преступлениях японских войск во время интервенции. В списке атакуемых оказались ведущие Министерства и ведомства, сайты крупнейших японских корпораций и сайты, посвященные Второй мировой войне. При этом китайские хакеры продемонстрировали высокий уровень организованности, о чем свидетельствует синхронность и массовость их атак.

В истории развития Интернет-преступности, таким образом можно выделить, на наш взгляд, несколько этапов:

I этап. Появление и становление Интернет как глобальной сети. В это время Интернет-преступность отсутствует как явление. Этап характеризуется отдельными деяниями, которые несли общественную опасность.

II этап. Становление Интернет-преступности. Появление субкультуры хакеров. Количественный рост преступности в глобальной сети. Пока Интернет-преступления совершаются лишь узким кругом специалистов. Появление специализаций компьютерных преступников.

III этап. Интернет начинает использоваться для совершения традиционных преступлений, становясь подспорьем для совершения любых преступлений. Широкая общественная распространенность Интернет-преступлений в отдельных странах, появление крупных национальных «хакерских групп».

IV этап. Преступность в Глобальной сети носит уже транснациональный характер. Появление кибертерроризма, международных хакерских группировок во всех сферах Интернет-преступности. Сращивание транснациональной преступности и преступности в Глобальной сети. Использование Интернет в политических целях, возникновение таких явлений, как Интернет-забастовка и Интернет-война.

V этап. Прогнозируется, что при таких темпах роста Интернет-преступность будет преобладать над другими видами и будет обширно влиять не только на экономические, но и политические процессы. Но возможна стабилизация роста и контролируемая динамика Интернет-преступности в случае успешного противодействия ей.

Представляется, что в зависимости от характера развития цифровых информационных структур, а также от уровня технической

грамотности в стране по-разному протекает эволюция Интернет-преступности и законодательства, регулирующего сеть. Сложно установить общие временные рамки для данного процесса, так как в отдельно взятых странах эти этапы проходили в разные годы. То есть в соответствии с этапами развития Интернет-преступности должно происходить и развитие законодательства. Так, в этом процессе можно выделить некоторые последовательные этапы:

I этап. Полное отсутствие законодательства в области Интернет и компьютерных преступлений соответствует первому этапу эволюции Интернет-преступности — ее становлению. В это время против преступлений, совершенных посредством Интернет, пытались применять уже существующие статьи.

II этап. Принятие первых специализированных законов, касающихся компьютерных и Интернет-преступлений в ответ на количественный рост общественно опасных деяний в Глобальной сети (II этап развития Интернет-преступности).

III этап. Законодательство в сфере компьютерных преступлений становится самостоятельной областью, ужесточаются санкции за уже криминализованные деяния, что связано с резким ростом Интернет-преступности (III этап развития Интернет-преступности).

IV этап. Возникновение международных правовых актов, регулирующих отношения в сети Интернет и направленных на противодействие преступности в Глобальной сети. Такие меры стали необходимы в связи с выходом Интернет-преступности на международный уровень.

В силу того, что законодатели разных стран не могли не реагировать на вызовы, исходящие от Интернет-преступности, в соответствии с появлением и развитием тех или иных явлений в сетевой преступности происходили изменения как в национальных уголовных законах, так и в международных правовых актах. Так как Интернет-преступность зародилась и быстрее развивалась в США, то первым законом, противодействующим преступности в Интернет, стал «Закон о компьютерном мошенничестве и злоупотреблениях», принятый в 1986 г[15]. Представляется, что Интернет-преступность в США в это время находилась на этапе становления (II этап развития). В России в это время сеть Интернет отсут-

[15] См: Federal Criminal Code and rules / Title 18 — Crime and Criminal Procedure. West Supp. — 1999. § 1030.

ствовала как таковая, поэтому о зарождении сетевой преступности, а тем более о появлении законодательства в этой области в то время еще не было и речи.

Когда в остальных развитых странах принимают первые законы (Computer Misuse Act 1990. London — в Великобритании, 1993 г. — Голландия[16]), в США Интернет становится не только средством совершения специфических преступлений, но и серьезным подспорьем для традиционных преступлений[17]. В связи с этим в 1996 г. ужесточаются санкции за 7 типов компьютерных преступлений: 1) несанкционированный доступ для получения секретной государственной информации с целью нанести урон США или для выгоды другого государства; 2) несанкционированный доступ к компьютеру для получения защищенной финансовой или кредитной информации; 3) несанкционированный доступ к компьютеру, который используется федеральным правительством; 4) несанкционированный доступ к компьютерной системе без разрешения или сверхполномочий с целью совершить мошенничество и т. д.[18]. Это время можно считать началом третьего этапа развития Интернет-преступности и борьбы с ней посредством принятия соответствующих законов.

В последующие годы происходила интеграция Интернет-преступности отдельных государств в единую общемировую преступность. На этом этапе сетевая преступность в США уже не так явно опережает преступность в других странах. Появляются новые очаги Интернет-преступности мирового масштаба — это некоторые европейские (Германия, Великобритания) и азиатские страны (Китай, Ю. Корея, Япония). В это время и принимаются первые международные правовые акты в рамках уже межгосударственного противодействия Интернет-преступности. Первой попыткой наведения порядка в сети принято считать специальную Конвенцию по борьбе с киберпреступностью, подписанную в 2001 г. в Будапеште представителями 30 государств — членов совета Европы.

---

[16] Уголовный кодекс Голландии / Под ред. Б.В. Волженкина. — СПб.: Юридический центр Пресс, 2000.

[17] Ляпунов Ю. Ответственность за компьютерные преступления / Ю. Ляпунов, В. Максимов // Законность. — 1997. — № 1. — С. 8—9.

[18] Геллер А.В. Уголовно-правовые и криминологические аспекты обеспечения защиты электронной информации и Интернета: дис. ... канд. юрид. наук: 12.00.08. — М., 2006. — С. 142.

История развития Интернет-преступности в России имеет определенные отличия. Это, прежде всего, связанно с некоторой запоздалостью (примерно на 15 — 20 лет) появления сети Интернет в России, но в то же время высоким техническим уровнем ее компьютерщиков, что позволило очень быстро пройти первые три этапа развития преступности в сети — буквально за 10 лет (в США за 30 лет). В настоящее время российская Интернет-преступность тесно интегрирована в мировую преступность в Глобальной сети, хотя в относительных и абсолютных показателях она пока еще не достигает уровня США, стран ЕС и некоторых азиатских стран в силу сравнительно низкой интернетизации населения, но уже имеет такую же сложную структуру и большое количество преступных специализаций. Кроме того, Россия является лидером в некоторых видах Интернет-преступности, таких как нарушение авторских и смежных прав, спам и распространение порнографии (в том числе детской). Несмотря на это, законодательство в области компьютерных и Интернет-преступлений находится на втором этапе развития и не может эффективно противостоять вызову, брошенному таким динамичным негативным явлением, как Интернет-преступность.

Интернет-преступность не стоит на месте, появляются все новые и новые виды преступлений, совершенных посредством Интернет. Появление Интернет привело не только к изменению традиционных преступлений, таких как мошенничество, вымогательство, убийство, но и к созданию новых видов преступлений, — например, незаконному доступу к информации или распространению вредоносных программ. Хотя совершение новых видов преступлений может осуществляться и без Интернет (заражение компьютерным вирусом с дискеты), но Интернет за счет глобальности, анонимности, быстроты транзакций послужил переходу данных преступлений в новое качество. Заметим, что этапы развития, выделенные в монографии, проходит Интернет-преступность в любой стране, меняются лишь быстрота прохождения того или иного этапа, но порядок остается тем же. Несмотря на отставание российской Интернет-преступности в прошлом, констатируем, что в настоящее время национальная преступность в Глобальной сети успешно интегрирована в международную Интернет-преступность и находится на четвертом этапе развития.

1.2. Интернет как способ и средство совершения преступлений

Начиная любую научную работу, необходимо сформулировать базовый набор понятий и определений. Ключевым термином при изучении Интернет-преступности является собственно «сеть Интернет». В Российской юридической энциклопедии определено, что Интернет — международная сеть соединенных между собой компьютеров, уникальное средство всемирной коммуникации[19]. И. М. Рассолов определяет Интернет в свете теории права как, прежде всего, новое пространство человеческого самовыражения; международное пространство, пересекающее любые границы; децентрализованное пространство, которым никакой оператор, никакое государство полностью не владеет и не управляет[20]. На наш взгляд, данная формулировка скорее подчеркивает международную и социальную значимость Интернет, но не затрагивает его свойств и особенностей, кроме разве что транснациональности. Некоторые авторы рассматривают Интернет как одну из разновидностей глобальных сетей, отмечая, что Интернет является конгломератом большого числа глобальных сетей, подчиняющихся некоторым общим правилам. В силу чего здесь наиболее ярко проявляются практически все тенденции, связанные с функционированием современных глобальных компьютерных сетей[21] . Данное определение скорее более техническое и структурное, не отражающее, чем Интернет принципиально отличается от других технологий связи и компьютерных сетей.

В целом же ученые пытаются избегать собственных определений сети Интернет, предпочитая пользоваться чисто техническим[22]

---

[19] Российская юридическая энциклопедия. — М.: Издательский Дом ИНФРА-М, 1999. — С. 380.

[20] Рассолов И.М. Право и Интернет. Теоретические проблемы. — М.: Изд-во НОРМА, 2003. — С. 92.

[21] См: Осипенко А.Л. Борьба с преступностью в компьютерных сетях: Международный опыт: Монография. — М.: Норма, 2004. — С. 15; Красненкова Е.В. Обеспечение информационной безопасности в Российской Федерации уголовно-правовыми средствами: дис. ... канд. юрид. наук: 12.00.08. — М., 2006. — С. 133.

[22] Казарян Э.А. Совершенствование правового регулирования распространения информации в Интернете: дис. ... канд. юрид. наук: 12.00.14. — М., 2004. — С. 87.

определением, либо вообще обходят этот вопрос стороной, выделяя только некоторые свойства[23]. Например, в работе Т.П. Кесареевой «Криминологическая характеристика и проблемы предупреждения преступности в Российской сети Интернет», так и не дано ее определение ни на одной из 195 стр. монографии.

Интернет не изначально проектируемая целиком система, а объединение множества компьютерных сетей, на основе протокола IP (Internet protocol) и протокола маршрутизации пакетов данных. В результате такого объединения сетей образуется глобальное информационное пространство, которое связывает ЭВМ, системы ЭВМ и сети ЭВМ по всему миру. То есть несмотря на то, что Интернет имеет конкретное физическое воплощение: компьютеры, линии связи, серверы, Глобальная сеть, — это, прежде всего, договор (протокол), который унифицирует обмен данными в цифровом представлении между компьютерами и компьютерными сетями. Это позволяет компьютерам, произведенным для разных целей, разными компаниями, с разными характеристиками без проблем передавать друг другу данные в электронном виде, так как правила передачи задокументированы и строго определены.

Получается, что, с одной стороны, Интернет — это множество компьютеров, соединенных в единую сеть, и структура, реализованная в материальном мире. С другой стороны, как и множество пчел это не рой, а множество преступлений не преступность, так и говорить, что Интернет это просто множество компьютеров, нельзя. Глобальная сеть — это, прежде всего, набор абстрактных принципов и задокументированных протоколов, а уже потом реализованная на их основе глобальная система взаимодействия компьютеров. Можно выделить три уровня абстракции Интернет. Во-первых, это собственно уровень идей коммуникации компьютеров, таких как независимость, надежность, глобальность, универсальность и т.д. Во-вторых, это уровень стандартизации этих идей или формальный уровень — уровень протоколов, описывающих спецификации взаимодействия. И третий уровень — это физическая реализация идей на основании протоколов.

---

[23] Геллер А.В. Уголовно-правовые и криминологические аспекты обеспечения защиты электронной информации и Интернета: дис. ... канд. юрид. наук: 12.00.08. — М., 2006. — С. 14—46.

В свою очередь протоколы Интернет это также многоуровневая система. Самый нижний уровень это протоколы физической реализации (физический уровень), которые описывают реализацию конкретных соединений, например, какова максимальная и минимальная сила сигнала или как должен защищаться провод от помех. На этом уровне протоколы Интернет ничем не отличаются от протоколов, скажем, телерадиовещания. Выше располагается уровень протоколов, отвечающих за передачу данных между двумя компьютерными системами (канальный уровень).

Одним из определяющих облик современной глобальной сети является сетевой уровень, IP (Internet Protocol, межсетевой протокол) обеспечивает на маршрутизацию и доставку без установления соединений. В IP используется коммутация пакетов и выполняется поиск оптимального способа их передачи. Отметим, что этот процесс абсолютно обезличен и адресат пакета может быть установлен только по Интернет адресу (IP - адрес), более того не существует какого то строгого маршрута следования, поэтому пакеты на которое бьется сообщение может быть передано по разным путям следования. Тесно связан с сетевым уровнем вышестоящий транспортный уровень, например на этом уровне находится протокол TCP, одной и функций которого является гарантированная доставка IP-пакетов. Вышестоящие уровни во многих моделях[24] относятся к прикладным функциям Интернет.

Важным свойством такой иерархии является, что каждый вышестоящий уровень наследует свойства нижестоящего, так как сообщение, отправленное с верхнего уровня, проходит все нижние уровни и то есть все равно ограничено рамками более нижних уровней.

Интернет как набор протоколов — это динамическая система, которая непрерывно меняется, причем изменения инициируются как сверху вниз (от объединений и консорциумов), так и снизу вверх (отдельные компании и разработчики). Сначала анализируются преимущества тех или иных нововведений, потом создаются

[24] Существуют разные модели уровней, где те или иные протоколы относятся к разным уровням, но порядок уровней везде одинаковый, хотя в некоторых их количество различается. Отметим, что есть аналоги TCP/IP, но сейчас они мало распространены и поэтому не описаны в работе.

и документируются стандарты вводимой технологии, а потом производители техники и программного обеспечения реализуют «ноу хау». Также распространен и обратный вариант, что разработчики пытаются сделать общеупотребительными свои внутренне стандарты. Несмотря на появление новых протоколов и технологий, основой Интернет все равно является набор идей, заложенных изначально при создании прообраза Глобальной сети APRAnet.

Более того, двойственную природу имеет и информация. С одной стороны, информация — это какие-либо данные об объектах и процессах внешнего мира. С другой — информация в компьютерных технологиях это еще и ее реальное воплощение. Кроме этого существуют виды цифровой информации, которые выделяются из остального ряда информации. Это метаинформация или информация об информации, с помощью которой задаются структура и связи в электронной информации, а также функциональная информация или алгоритмы — информация о способах обработки информации. Несмотря на кажущуюся отвлеченность вышеприведенных рассуждений, заметим, что данный факт имеет важное прикладное значение. Получается, что преступник, выбирая информацию как предмет преступления, или используя манипуляции с информацией как прием для достижения своей преступной цели может оперировать на совсем разных уровнях. Так, изменение обычной информации хотя и может повлечь значительные негативные последствия, то незаконная модификация метаинформации и функциональной информации уже таит в себе скрытый и трудноценимый вред.

В связи с такой многоликостью Интернет и информации, объединенной при помощи Интернет в глобальное информационное пространство, встает вопрос, какое место может занимать Интернет в преступлении. Для выяснения данного вопроса необходимо отметить, что Интернет может применяться на всех стадиях преступления: приготовление, покушение, оконченное общественно опасное деяние. Кроме этого использование Интернет может различаться по интенсивности и влиянию на наступление преступного результата. Интернет может быть применен для получения информации, облегчающей совершение преступления, например, сведений о том, как создать взрывное устройство или изготовить сложный синтетический наркотик в домашних условиях. В данном случае Интернет задействован крайне не интенсивно, и хотя пре-

имущества, получаемые при выборе перспективной технологии очевидны, но преступник может получить информацию и из других каналов. То есть применение Интернет не сильно влияет на наступление преступного результата.

С другой стороны, Глобальная сеть может применяться для распространения порнографии за рубежом, при этом делать это вопреки уголовному закону каким-либо другим способом достаточно тяжело. В таком случае Интернет используется крайне интенсивно как для нахождения покупателей, моделей и т.д., так и для пересылки собственно материала и получения за него денежных средств, т.е. используется непосредственно для совершения общественно опасного деяния. Именно использование Глобальной сети позволяет в данном случае создать расширенную сеть сбыта и способствует наступлению преступного результата, оставляя эту деятельность вне поля зрения правоохранительных органов.

Заметим, что, независимо от «интенсивности» и влияния на наступление преступных последствий, в обоих случаях Интернет выступал в качестве средства, то есть предмета материального мира или процесса, используемого для совершения преступления путем непосредственного воздействия на объект посягательства, так и для действий вспомогательного характера, входящих в объективную сторону преступления[25].

Представляется, что и при использовании Интернет для непосредственного воздействия на объект, и при выполнении действий вспомогательного характера Глобальная сеть является признаком объективной стороны (средством). Хотя при этом очень важно отметить разные оттенки этого понятия. В том случае, когда Интернет используется как средство для совершения действий второстепенного плана, можно говорить о совершении преступлений с использованием Интернет. А когда само преступное деяние совершается с помощью Интернет, следует говорить о собственно совершении преступления посредством Интернет.

Данное разделение имеет не только формальный, но и прикладной характер. Когда речь идет об использовании Интернет для совершения второстепенных действий, то тут очевидна схожесть с другими введенными в преступный оборот технологиями. Как в

[25] Парфенов А.Ф. Общее учение об объективной стороне преступления: дис. ... канд. юрид. наук: 12.00.08. — СПб., 2006. — С. 169.

свое время использование автомобиля, телефона или компьютера позволило ускорить этап приготовления к преступлению и сократило многие временные и материальные затраты, так и Интернет позволяет сократить этап его приготовления и удешевляет многие предваряющие преступление операции. В свою очередь, возможность совершения непосредственно общественно опасного деяния посредством Интернет изменила само его качество: преступление благодаря Глобальной сети стало анонимным, удаленным в пространстве, трансграничным, глобальным. Интернет разделил место совершения преступных действий и место наступления последствий, а также сделал выявление, пресечение и уголовное преследование преступлений чрезвычайно трудным, а в ряде случаев невозможным.

То есть при совершении самого преступного деяния посредством Интернет можно говорить, что применена новая совокупность приемов, методов, последовательности действий, которая придает преступлению уникальные свойства, не характерные для преступлений без использования Интернет.

Представляется, что в такой трактовке совершение преступления посредством Интернет является и способом преступления[26], и в то же время Интернет является средством как совокупность предметов и процессов материального мира. Такое двойственное его значение при совершении преступления возможно благодаря природе самого Интернет, который является одновременно набором принципов, алгоритмов, правил взаимодействий и в то же время он реализован в материальном мире в виде совокупности соединенных компьютеров.

Получается, что в случаях, когда Интернет непосредственно используется для совершения преступления, он является способом и средством одновременно, а в остальных — лишь средством. Заметим, что при совершении самого общественно опасного деяния посредством Интернет изменяются его характеристики. За счет того, что Глобальная сеть обладает уникальными возможностями, изменяется качество преступления, что не может не отразиться на степени его общественной опасности.

---

[26] Уголовное право Российской Федерации. Общая часть: Учебник для вузов / Под ред. А.И. Рарога, А.С. Самойлова. — М.: Высшее образование, 2005. — С.144.

Представляется, что когда речь об Интернет идет как о способе преступления, имеется ввиду не физическая реализация, то есть не множество компьютеров, соединенных километрами проводов, а подразумевается набор принципов и правил, которые легли в основу функционирования сети. Эти принципы выражены формальным языком в протоколах, описывающих взаимодействие реально существующей сети. Основными протоколами, определяющими современный облик сети, являются несомненно IP (Internet Protocol) и TCP (протокол маршрутизации). Любые сети, реализованные на основе этих протоколов, также обладают свойствами и принципами сети Интернет, отличаясь зачастую лишь распространенностью и общедоступностью. Например, сеть VPN (Virtual Private Network — Виртуальная приватная сеть), хотя обеспечивает более высокий уровень защищенности и ограничивает доступ посторонних адресатов, эта защищенность ограничена рамками протоколов, которые лежат в основе ее маршрутизации и адресации, то есть рамками IP и TCP[27]. Представляется, что называть не Интернет-сетью сеть, построенную на основе протокола IP, который дословно переводится как «Интернет протокол», не совсем корректно. То есть к Интернет-преступлениям относятся любые преступления, в которых Интернет используется как средство, но в этом массиве особенно выделяются деяния, где Интернет это не только средство, но и способ, так как при использовании Глобальной сети для совершения непосредственно общественно опасного деяния изменяются не только количественные характеристики (время приготовления и стоимость приготовительных действий), но и качественные (общественная опасность, анонимность, трансграничность).

1.3. Понятие Интернет-преступности

В условиях активно формирующегося законодательства в области компьютерных технологий, информации и сети Интернет проблема выработки терминологии приобретает особую важность.

---

[27] Новак Д. Обнаружение нарушений безопасности в сетях, 3-е издание.: Пер. с англ / Д. Новак, С. Норткат. — М.: Издат. дом «Вильямс», 2003. — С. 25—43.

В силу специфики данных вопросов в исследуемой области используются термины, заимствованные из технических дисциплин. В обстановке непрерывно развивающихся компьютерных технологий такое заимствование для регулирования новых формирующихся отношений вполне обоснованно и необходимо. При этом специальные термины должны не только отражать понятие, но и быть в той или иной степени признанными как в технической, так и в юридической науках.

Когда авторы говорят об Интернет-преступности и Интернет-преступлениях, они применяют целый набор терминов, среди них: «компьютерная преступность и преступления[28]», «преступность в области компьютерной информации», «преступления в сфере высоких технологий», «преступность в сети Интернет», «киберпреступность»[29], даже «информационная преступность»[30], «информационные компьютерные преступления»[31] и т. д.

Сеть Интернет не единственная глобальная сеть, а Интернет не единственная технология, создаваемая на основе компьютерной техники. Чтобы отделить Интернет-преступность от других видов противоправных деяний, нам необходимо хорошо представлять особенности сети Интернет не только как технологии, но и как социально-информационного и субкультурного явления, а также важно понимать, что Интернет — это прежде всего набор правил и принципов, которые задокументированы в протоколах и реализованы на практике.

При этом наиболее широкое из всех употребляемых в научно-правовой литературе понятий термин «компьютерная преступность». Например, Д.В. Добровольский определяет «компьютер-

---

[28] Комментарий к Уголовному кодексу Российской Федерации с постатейными материалами и судебной практикой / Под общ. ред. С.И. Никулина. — М.: Изд-во «Менеджер»; Изд-во «Юрайт», 2001. — С. 883.; Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. В.И. Радченко; Науч. ред. А.С. Михлин. — М.: Спарк, 2000. — С. 647.

[29] Войниканис Е.А. Информация. Собственность. Интернет: традиция и новеллы в современном праве. — М.: Волтерс Клувер, 2004. — С. 65.

[30] Горшенков Г.Н. Киберкриминология: к понятию «информаионная преступность» // Российский криминологический взгляд. — 2005. — № 4. — С. 93—96.

[31] Российское уголовное право. Курс лекций. Т.5. Преступления против общественной безопасности и общественного порядка / Под ред. проф. А.И. Коробеева. — Владивосток: Изд-во Дальневост. ун-та, 1999. — С. 577.

ную преступность» как совокупность преступлений в сфере «информационных технологий»[32]. Он утверждает, что недопустимо включать в компьютерные преступления только общественно опасные деяния, предметом которых является компьютерная информация.

Эти положения подтверждает и А.А. Жмыхов, говоря о том, что компьютерная преступность — это совокупность преступлений, совершаемых с помощью компьютерной системы или сети, в рамках компьютерной системы или сети и против компьютерной системы или сети. Он утверждает, что кроме преступлений в сфере компьютерной информации, компьютерными преступлениями также являются и преступления, связанные с компьютерами. То есть такие традиционные по характеру преступные деяния, совершенные с помощью вычислительной техники, как кража, мошенничество, причинение вреда и некоторые другие, за которые предусматриваются уголовные санкции в законодательствах большинства стран[33]. Существует и более широкая трактовка, так группа экспертов Организации экономического сотрудничества и развития (ОЭСР) в 1986 году дала определение компьютерного преступления, под которым понималось любое незаконное, неэтичное или неразрешенное преступление, поведение, затрагивающие автоматизированную обработку и (или) передачу данных[34]. Представляется, что такое определение было актуально 20 лет назад, когда компьютерная техника была редкостью, но теперь, когда средства автоматизированной обработки данных используются повсеместно, то данное понятие охватывает огромный круг деяний, так например сотовый телефон тоже средство передачи.

Термин «компьютерная преступность» признается и за рубежом, в ряде стран, на государственном уровне. Например, подразделение при департаменте юстиций США, занимающееся компьютерными преступлениями и преступлениями против интеллектуальной собственности, так и называется «Отдел компьютерных

---

[32] Добровольский Д.В. Актуальные проблемы борьбы с компьютерной преступностью: дис. ... канд. юрид. наук: 12.00.08. — М., 2005. — С. 45—46.

[33] Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение: дис. ... канд. юрид. наук: 12.00.08. — М., 2003. — С. 18—19.

[34] Малыковцев М.М. Уголовная ответственность за использование и распространение; вредоносных программ для ЭВМ: дис. ... канд. юрид. наук: 12.00.08. — М., 2006. — С. 13.

преступлений и интеллектуальной собственности» (англ. Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice)[35]. В США термин компьютерное преступление (Computer Crime) возник около 1940 г.[36], то есть имеет относительно длинную историю, по сравнению с другими понятиями в области компьютерной преступности.

В литературе высказывалась точка зрения, что термин «компьютерное преступление» гораздо шире понятия «преступление в сфере компьютерной информации»[37]. Мы также разделяем это мнение, так как любая компьютерная информация не отделена от компьютера или сети компьютеров, следовательно, любое преступление в сфере компьютерной информации — это компьютерное преступление. Кроме этого к компьютерным преступлениям могут относиться традиционные преступления, совершенные с помощью компьютерной техники, так как использование новейших технологий позволило выйти данным видам общественно опасных деяний на новый уровень.

Компьютерные преступления и компьютерная преступность понятия криминологические, так как в УК РФ такого термина нет, хотя глава «Компьютерные преступления» была в проекте УК РФ 1995 г.[38] . Компьютерная преступность, в свою очередь, — это совокупность преступлений, где компьютерная информация является предметом преступных посягательств, а также преступления, которые совершаются посредством общественно опасных деяний,

---

[35] См. также: Степанов-Егиянц В.Г. Ответственность за компьютерные преступления // Законность. — № 12. — 2005. — С. 49; Малыковцев М.М. Уголовная ответственность за использование и распространение; вредоносных программ для ЭВМ: дис. ... канд. юрид. наук: 12.00.08. — М, 2006. — С. 13; Мазуров В.А. Компьютерные преступления: классификация и способы противодействия. — М.: Палеонтип, 2002. — С. 5—6.

[36] Ястребов Д.А. Институт уголовной ответственности в сфере компьютерной информации (опыт международно-правового сравнительного анализа) // Государство и право. — 2005. — № 1. — С. 53.

[37] Зыков Д.А. Виктимологические аспекты предупреждения компьютерного мошенничества: дис. ... канд. юрид. наук: 12.00.08. — Владимир, 2002. — С. 17.; Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение: дис. ... канд. юрид. наук: 12.00.08. — М., 2003. — С. 18.

[38] Айсанов Р.М. Состав неправомерного доступа к компьютерной информации в российском, международном и зарубежном уголовном законодательстве: дис. ... канд. юрид. наук: 12.00.08. — М., 2002. — С.20.

предметом которых является компьютерная информация[39]. Заметим, что при таком определении умышленный поджог компьютерного сервера с целью уничтожить важную информацию также является компьютерным преступлением, так как одним из предметов преступления является компьютерная информация. С другой стороны, отключение аппарата вентиляции легких с помощью компьютерной сети человеком, имеющим легальный доступ, например, техником больницы или доктором, и повлекшее смерть пациента, не является компьютерным преступлением, так как все операции с компьютерной информацией в этом случае абсолютно легальны.

Хотя в УК РФ термина «компьютерное преступление» нет, в законе используется понятие «компьютерная информация», так, Глава 28 УК РФ носит название «Преступления в сфере компьютерной информации» и содержит статьи, криминализующие соответствующие деяния: «Неправомерный доступ к компьютерной информации» (ст. 272 УК РФ); «создание, использование и распространение вредоносных программ для ЭВМ» (ст. 273 УК РФ); «нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» (ст. 274 УК РФ). Однако вряд ли в современных условиях можно считать это полным списком преступлений в сфере компьютерной информации.

Например, С.Д. Бражник считает, что круг криминализованных деяний в Главе 28 УК РФ надо расширить, включив в нее компьютерный шпионаж, компьютерный терроризм, компьютерное мошенничество, причинение имущественного вреда путем изменения компьютерной информации и т. д[40]. Такая возможность не исключена, так как законодательная база, регулирующая отношения в сфере компьютерной информации и информационной безопасности, находится на этапе становления и совершенствования. Особенно это касается отношений, возникших в результате появления сети Интернет, а также в силу таких особенностей этой технологии, как глобальность, анонимность, широкая распространенность и т.д.

---

[39] Криминология: Учебник для вузов / Под общ. ред. д.ю.н. проф. А.И. Долговой. — 2-е изд., перераб. и доп. — М.: Изд-во НОРМА, 2003. — С. 673—675.

[40] Бражник С.Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: дис. ... канд. юрид. наук: 12.00.08. — Ижевск, 2002. — С. 157—161.

М.С. Гаджиев в рамках криминолого-криминалистического подхода использует понятия «компьютерное преступление» и «преступление в сфере компьютерной информации» как эквивалентные[41]. Представляется, что понятие «компьютерное преступление» охватывает как преступления в сфере компьютерной информации, так и другие компьютерные преступления.

Можно встретить в работах российских авторов и такое определение, как «киберпреступность», которое достаточно часто употребляется за рубежом[42]. Так, Т.Л. Тропина считает, что понятие «компьютерная преступность» недостаточно для охвата всех деяний, совершаемых при помощи вычислительной техники, глобальных сетей. Киберпреступность, по ее мнению, — это совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей или компьютерных данных[43].

Представляется, что требуется рассмотреть это понятие поподробней. Компьютерные данные — это одна из разновидностей компьютерной информации. А компьютерная информация является, в свою очередь, неотъемлемой частью компьютерной системы[44]. Конечно, компьютерная информация может существовать и вне компьютерной системы, например, на дискете, но все операции с нею можно производить только с помощью компьютера.

---

[41] Гаджиев М.С. Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан): дис. ... канд. юрид. наук: 12.00.08. — Махачкала, 2004. — С. 19.

[42] См. например: Sinrod E.J., Reilly W.P. Cyber-Crimes: A practical approach to the application of federal computer crime laws // Santa Clara computer and high technology law journal. — Vol. 16. — № 2. — P. 3.

[43] Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук: 12.00.08. — Владивосток, 2005. — С. 36.

[44] Вехов В.Б. Проблемы определения понятия компьютерной информации в свете унификации уголовных законодательств стран СНГ // Уголовное право. — 2004. — № 4. — С. 17; Шарков А.Е. Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации: дис. ... канд. юрид. наук: 12.00.08. — Ставрополь, 2004. — С. 27.

Доступность для восприятия ЭВМ служит одной из отличительных особенностей компьютерной информации[45].

Некоторые авторы относят внешние носители компьютерной информации и периферийные устройства к составляющим компьютерной системы[46]. Поэтому определение, данное Т.Л. Тропиной, представляется малофункциональным, так как все преступления против компьютерных систем и сетей можно свести к преступлениям против компьютерных данных. Даже физическое вмешательство в работу устройства все равно является операцией с данными. Так, например, если злоумышленник перерезал провод, по которому передаются данные, то в рамках логического представления компьютерных сетей он просто нарушил передачу данных.

Получается, что термин «компьютерная преступность» все же более емкий, чем киберпреступность, используемый Т.Л. Тропиной. Согласно А.А. Жмыхову, как упоминалось выше, компьютерная преступность — это совокупность преступлений, совершаемых с помощью компьютерной системы или сети, в рамках компьютерной системы или сети и против компьютерной системы или сети. Отличительным признаком киберпреступности от определения А.А. Жмыхова компьютерной преступности является характеристика совершения таких преступлений в *киберпространстве*. Если исходить из этой трактовки киберпреступности, то понятие компьютерная преступность гораздо шире, так как компьютерные преступления — это **все** преступления, совершаемые с помощью или посредством компьютерных систем или компьютерных сетей, а не только преступления, совершенные в киберпространстве.

Вообще термин «киберпространство» был предложен впервые писателем фантастом Вильямом Гибсоном, который употреблял его для обозначения пространства, образуемого компьютерными сетями[47] . Даже если понимать «киберпреступность» в том смыс-

---

[45] Вехов В.Б. Правовые и криминалистические аспекты понятия компьютерная информация // «Черные дыры» в российском законодательстве. — 2004. — № 3. — С. 243.

[46] Ушаков С.И. Преступления в сфере обращения компьютерной информации (теория, законодательство, практика): дис. ... канд. юрид. наук: 12.00.08. — Ростов-на-дону, 2000. — С. 52.

[47] Mungo P. The Extraordinary underworld of Hackers, Phreakers, Virus writers, and Keyboard criminals / P. Mungo, B. Clough. — New york: Random house, 1992. — P. 200—202.

ле, в котором его употребляют в США и Великобритании, то есть все преступления, совершенные с помощью компьютеров и средств телекоммуникации, то данному заимствованному иностранному термину можно найти русский аналог, который уже широко употребляется, — это «Преступления в сфере телекоммуникаций и компьютерной информации».

Представляется, что целесообразность использования термина «киберпространство» и «киберпреступность» в российской криминологической науке пока под вопросом, тем более, что уже есть термины, которые используются в России более 10 лет.

Преступность в сети Интернет, которая является частью компьютерной преступности, уже выделялась в некоторых работах как отдельный вид преступности. Т.П. Кесареева, например, в своей работе делает вывод о том, что преступность в сети Интернет является неотъемлемой частью компьютерной преступности, обладающей своими специфическими особенностями. Под преступностью в Интернет следует понимать запрещенные уголовным законом общественно опасные деяния, совершенные путем вхождения в сеть Интернет с использованием средств компьютерной техники, подключенных к сети Интернет[48]. Представляется, что это определение перегружено лишними терминами, так как любое вхождение в сеть Интернет происходит с использованием компьютерной техники, подключенной к сети Интернет.

И.М. Рассолов также выделяет преступность в сети Интернет в отдельный вид преступности, хотя и использует понятия «преступность в Интернет», «киберпреступность», «компьютерная преступность» как синонимы[49]. Он также выделяет Интернет-право в отдельную отрасль права, как и некоторые другие авторы[50]. Это выделение вполне обоснованно, так как Интернет как новый спо-

---

[48] Кесареева Т.П. Криминологическая характеристика и предупреждение преступности в российском сегменте сети Интернет: дис. ... канд. юрид. наук: 12.00.08. — М., 2002. — С. 56.

[49] Рассолов И.М. Право и Интернет. Теоретические проблемы. — М.: Изд-во НОРМА, 2003. — С. 251—253.

[50] См., например: Михайленко Е.В. Информационное право в свете развития глобальной сети Интернет // Закон и право. — 2004. — № 8. — С. 61; Тедеев А.А. Информационное право (право Интернета): Учебное пособие. — М.: Изд-во Эксмо, 2005. — С. 8—9.

соб взаимодействия породил общественные отношения особого вида. Интернет-торговля, Интернет-общение, Интернет-работа существенно отличаются от не Интернет аналогов в силу особенностей сети Интернет, описанных в предыдущем параграфе. Например, Интернет породил новые отношения в сфере труда, когда «неофициальный» работодатель, даже не видел в лицо работника, когда они могут быть разделены границами и огромными расстояниями и т.д.

Важным вопросом остается, по какому признаку выделять новые виды преступлений, связанных с компьютерной техникой. Представляется, что выделение «компьютерных преступлений», «Интернет-преступлений», «киберпреступлений» на основании предмета преступления не совсем корректно, так как тогда в данные классы деяний попадают и преступления, ничем не отличающиеся от традиционных, — например, поджог компьютерной системы. Предметом в данном случае является компьютерная система, но преступления такого рода незачем выделять в отдельный вид. Или, например, кража носителя компьютерной информации, совершенная с помощью отвертки путем откручивания этого носителя от компьютера.

Не совсем оправданно предложение выделения новых технологических видов преступления с помощью места их совершения. Так, например, Т.Л. Тропина выделяет «киберпреступления» как преступления, совершенные с помощью или посредством доступа к моделируемому с помощью компьютера информационному пространству[51]. Заметим, что очертить границы моделируемого с помощью компьютера информационного пространства достаточно сложно. Во-первых, с помощью компьютера моделируется несколько уровней информационных пространств в силу иерархичности самой информации (см. § 1.2.): информация, инструментальная информация и метаинформация — каждый из этих уровней относительно независим. Во-вторых, с помощью компьютера моделируются информационные пространства: Интернет-телевидение, Интернет-телефония, Интернет-радиотрансляция — ничем функционально не отличимые от ранее существующих.

---

[51] Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук: 12.00.08. — Владивосток, 2005. — С. 38.

Т.П. Кесареева выделяет преступления в сети Интернет как преступления, совершенные путем вхождения в сеть Интернет. Заметим, что никакого вхождения в действительности не происходит, а производится взаимодействие компьютерной техники и компьютерных сетей посредством принципов и алгоритмов, задокументированных в протоколах IP, TCP и других. Поэтому следует выделять компьютерные преступления, киберпреступления, Интернет-преступления как новый вид общественно опасных деяний по способу или средству совершения преступлений.

Исходя из анализа используемых в юридической литературе определений, предлагаем определения Интернет-преступления и Интернет-преступности, отвечающие современным реалиям. По нашему мнению, Интернет-преступления — это любые запрещенные уголовным законом общественно опасные деяния, совершенные посредством или с помощью Интернет. Сюда входят преступления, когда Интернет использовался на стадии приготовления к совершению преступления. Так, например, поиск средств компьютерного взлома по Интернет является Интернет-преступлением, хотя необходимо различать интенсивность использования в случае, когда Интернет является лишь средством и выступает в качестве способа. В преступлениях, где Интернет лишь средство, уже используются некоторые свойства Глобальной сети, но не в полной мере, — это переходный вид преступлений, который также относится к Интернет-преступлениям.

Необходимо сделать поправку на существенные различия в законодательствах по поводу установления ответственности за Интернет-преступления. Интернет-преступлением в конкретно взятой стране будет называться деяние, за которое предусмотрена уголовная ответственность именно в этой стране. Так, Интернет-преступление в России — это любое запрещенное УК РФ общественно опасное деяние, совершенное посредством или с помощью Интернет.

В свою очередь, российской Интернет-преступностью (или Интернет-преступностью в России) называется социально негативное явление, представленное в виде совокупности преступлений (запрещенных УК РФ деяний) и их системы, которые совершены посредством или с помощью сети Интернет с территории Российской Федерации, либо с территории других государств, но направленных против интересов Российской Феде-

рации. Представляется, что Интернет-преступления и Интернет-преступность имеют отличительные характеристики, дифференцирующие их от других видов противоправных деяний. Интернет-преступление характеризуется следующими свойствами: удаленность, неперсонофицированность, доступность. Интернет-преступность, в свою очередь, отличают крайне высокая латентность, интеллектуальность, транснациональность, быстрый рост. При этом необходимо выделить в качестве подвида такую наиболее опасную и качественно новую преступность, как совокупность преступлений, где Интернет является способом совершения преступлений, то есть используется непосредственно для совершения общественно опасного деяния.

Интернет-преступность является частью компьютерной преступности, если выделять компьютерную преступность по средству совершения, так как любое Интернет-преступление — это компьютерное преступление, но не наоборот. Не каждое преступление в сфере компьютерной информации является Интернет-преступлением, в тоже время такие традиционные преступления, как мошенничество, кража, вымогательство и другие, совершенные посредством Интернет, — это Интернет-преступления. При этом последствия не обязательно должны наступать в сети Интернет: например, убийство посредством остановки кардиостимулятора, подключенного в Глобальную сеть. Скажем, преступники проникли в локальную компьютерную сеть больницы, в которой содержался главный свидетель по громкому уголовному делу, и в результате посредством Интернет и при помощи специальных программ нарушили работу системы, контролирующей кардиостимулятор свидетеля. В итоге наступили негативные последствия в физическом качестве в виде смерти свидетеля.

Так как Интернет имеет логическую природу — это набор правил (протоколов) взаимодействия компьютеров в сети, то преступление, которое совершено без доступа Интернет, но с помощью Интернет-устройства, — например, удар частью компьютера по голове или поджег сервера при непосредственном контакте, не является Интернет-преступлением, так как не совершено посредством Интернет.

Представляется, что Интернет-преступность обладает некоторыми отличительными свойствами, характерными только для нее, в силу особенностей сети Интернет и быстрого развития инфор-

мационных технологий. Об этих особенностях Интернет-преступности и пойдет речь дальше.

1.4. Свойства Интернет-преступности и типология Интернет-преступлений

Общественно опасное деяние, совершенное с помощью сети, нередко попадает под несколько юрисдикций благодаря глобальной и межгосударственной природе Интернет[52]. В отличие от физического мира, где человек не может быть в нескольких местах в один момент времени, Глобальная сеть связывает сотни компьютеров по всему миру и позволяет виртуально присутствовать в нескольких местах одновременно, — например, вы можете со своего компьютера рассматривать картины Лувра и в то же время осуществлять мошеннические операции в Банке Нью-Йорка. Преступника и жертву нередко разделяют тысячи километров, так как нет различий в совершении преступления против компьютерных систем, расположенных на соседней улице или в другой стране, если вы совершаете преступление посредством Интернет. То есть в современных реалиях речь идет об *удаленности Интернет-преступлений.* Это свойство характерно также для всех не преступных действий, совершаемых с помощью Интернет.

Возникают серьезные сложности в определении субъекта Интернет-преступления. Механизмы идентификации глобальной сети позволяют личности совершать операции анонимно или выдавать себя за другое лицо, изменять биографические данные или социальный статус. При этом анонимность касается не только персо-

[52]The electronic frontier: the challenge of unlawful conduct involving the use of the Internet. A Report of the President's Working Group on Unlawful Conduct on the Internet [Электронный ресурс] / Департамент Юстиций США. — Режим доступа: http://www.usdoj.gov/criminal/cybercrime/unlawful.htm; Корнилс К. Локализация места ответственности за преступления, связанные с Интернетом // Право и информатизация общества. — М., 2002. — С. 299; Голубев В.А. Киберпреступность — угрозы и прогнозы [Электронный ресурс] / Центр исследования компьютерной преступности. — Режим доступа: http://www.crime-research.ru/articles/golubev_071

ны злоумышленника, но и его местонахождения, особенно, если преступник профессионал в сфере компьютерных технологий. Или компьютерная система, с которой пришел компьютерный вирус, могла быть сама подвержена воздействию вредоносных программ, и персонал, ее обслуживающий, мог об этом не знать, то есть распространение вируса происходило автоматизированно, и личность участвовала только в первом событии всей цепочки из тысячи звеньев. В настоящее время в Интернет существуют вредоносные программы, которые самостоятельно распространяются уже в течении многих лет, подобно вирусным заболеваниям. Все это свидетельствует *о неперсонофицированности и анонимности Интернет-преступлений.*

Неперсонофицированность и анонимность присутствует во всех отношениях и действиях, которые осуществляются посредством Интернет. Например, обезличенные знакомства в Интернет, что дает много преимуществ для контактеров, таких как возможность справится со своими комплексами, остаться незаметным для окружающих, если не хочется придавать огласке отношения и т.д. Для преступника анонимность и обезличенность позволяют выдать себя за другого человека, скрыться от правосудия, остаться вне общественного порицания и осуждения.

Совершение Интернет-преступления требует определенного набора знаний. Хотя планка уровня профессионализма понижается в связи с возможностью выполнять некоторые операции при помощи созданных другими людьми программных средств, которые легко найти в Интернет[53]. Несмотря на снижение уровня требований, необходимого для совершения преступления в сети, чтобы стать Интернет-преступником необходимо уметь работать с компьютером и Глобальной сетью, иметь представление об их физических и логических принципах работы. При этом некоторые преступники показывают, что они интеллектуально превосходят не только компьютерных специалистов из отдельных фирм, но и целые государственные службы. Так, известного компьютерного и Интернет-преступника Кевина Митника, который получил доступ к системам сотни компаний, среди которых Motorola, Novell, Fujitsu, Sun Microsystems, спецслужбы США не могли поймать в

[53] Например, существуют программы, находящие в сети незащищенные от неправомерного доступа и вирусов компьютеры.

течение 2,5 лет[54]. Сами хакеры говорят, что успех взлома зависит от интеллектуальных способностей[55]. Все это свидетельствует об *интеллектуальном характере Интернет-преступности.* Интеллектуальность среди компьютерных преступников пропагандируется также посредством субкультуры хакеров, что дает стимул Интернет-преступнику для умственного саморазвития.

Есть и другие виды преступлений, которые требуют определенных профессиональных знаний и интеллектуальных способностей, например, беловоротничковая преступность[56]. Но для совершения таких преступлений необходимо определенное социальное положение и достижение определенного возраста. Такие преступления раньше редко совершались людьми ограниченных физических и социальных возможностей. В свою очередь, компьютерные преступления, в частности Интернет-преступления, зачастую совершаются людьми, не достигшими совершеннолетия[57]. То есть данный вид преступлений не требует никаких иных способностей, кроме интеллектуальных. Можно сказать, что данные преступления, в отличие от других интеллектуальных преступлений, *доступны людям невысоких социальных и возрастных возможностей.* Для совершения Интернет-преступления не надо занимать высокое социальное положение, достаточно иметь доступ в Интернет и компьютер. С каждым годом услуги Интернет становятся все распространенней и дешевле, поэтому можно говорить, что исследуемые преступления станут еще доступней.

Еще один отличительный признак — это *высокая латентность Интернет-преступности*, как и всей компьютерной преступности. При этом авторы указывают разные причины этого феномена. Например, И.М. Рассолов называет одной из причин высокой скры-

---

[54] Kevin Mitnick sentenced to nearly four years in prison [Электронный ресурс] / Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice. — Режим доступа: http://www.cybercrime.gov/mitnick.htm

[55] Cornwall H. The hackers handbook. — E.A. Brown Co., 1986. — P. 42.

[56] Криминология / под. Ред. Дж. Ф. Шели; пер. с англ. — СПб.: Питер, 2003. — С. 343—347.

[57] It's Not Just Fun and «War Games» - Juveniles and Computer Crime [Электронный ресурс] / Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice. — Режим доступа: http://www.cybercrime.gov/usamay2001_7.htm

тости преступности в Интернет тот факт, что ущерб от преступления зачастую кажется жертве незначительным по сравнению с процедурой расследования, способной отнять время, но не гарантирующей привлечение к ответственности виновного и компенсации ущерба[58]. Также среди причин высокой латентности называют нежелание отдельных пользователей и компаний предоставлять правоохранительным органам доступ к своим конфиденциальным данным, что необходимо при некоторых расследованиях[59], и вариабельность конфигураций возможностей доступных преступнику в Интернет, быстрое развитие модификаций способов совершения[60]. Сложно точно оценить уровень латентности преступности в Интернет в силу неоднородности данного вида деяний, но существуют исследования, свидетельствующие о высокой латентности отдельных подвидов компьютерной и Интернет-преступности. Так, М.В. Старичков называет уровни латентности порядка 99,7% по ст. 272 УК РФ и 99,8% по ст. 273 УК РФ как для всех преступлений в сфере компьютерной информации, так и для преступлений в сфере компьютерной, совершенных посредством Интернет, хотя замечает, что полученные данные вряд ли могут претендовать на абсолютную достоверность[61].

Если еще 10 лет назад можно было говорить о привилегированности Интернет-преступности, и об ограниченном доступе к технологии Глобальной сети, сейчас одна четвертая всех россиян пользуется Интернет, а компьютерные преступления стали не такой уж и редкостью. Так, в 2006 г. в РФ зарегистрировано около 9000 преступлений в сфере компьютерной информации, что сопоставимо с количеством довольно-таки распространенных видов преступлений, например, «угоном» автотранспорта (в 2005 г. —

---

[58] Рассолов И.М. Право и Интернет. Теоретические проблемы. — М.: Изд-во НОРМА, 2003. — С. 251—254.

[59] Richard P. Salgado. Working with Victims of Computer Network Hacks [Электронный ресурс]/ Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice. — Режим доступа: http://www.cybercrime.gov/usamarch2001_6.htm

[60] Гаврилов М.В. Извлечение и исследование компьютерной информации / М.В. Гаврилов, А.Н. Иванов // Уголовное право. — 2004. — № 4. — С. 6.

[61] Старичков М. В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики : дис. ... канд. юрид. наук: 12.00.08. — Иркутск, 2006. — С. 109—112.

10058), «изнасилованием» (2006 г. — 8871) и т.д. Хотя по статьям Главы 28 УК РФ в официальной статистике последние два года роста не отмечается, быстро растет количество преступлений по другим статьям УК РФ (см. параграф «Состояние, структура и динамика Интернет-преступности в России»). Все это свидетельствует, во-первых, о *быстром росте Интернет-преступности*, во-вторых, о *широкой распространенности данного явления* в наши дни.

Среди признаков Интернет-преступности можно выделить также ее *транснациональный характер.* По мнению некоторых авторов, около 62% компьютерных преступлений совершается в составе организованных групп, находящихся, в том числе, на территории нескольких стран[62]. Например, преступные группировки, занимающиеся рекламой и распространением детской порнографии через Интернет, зачастую состоят из жителей различных стран СНГ и зарубежья. При этом соблюдается полная анонимность, взаимодействие происходит посредством Глобальной компьютерной сети через пароли и клички. Как правило, в лицо никто из участников друг друга не знает[63]. Посредством Интернет можно осуществлять многие трансграничные операции, особенно касающиеся передачи данных, чем и пользуются преступники.

Представляется, что в руках преступников Интернет — это удобное, быстрое и относительно безопасное средство для совершения преступлений любого рода. Свойства Интернет дают преимущества в совершении целого ряда преступлений, предоставляют новые преимущества организованной и международной преступности. Некоторые авторы даже сравнивают современную ситуацию со временами золотоискателей, когда провозглашается, что не применяются никакие правила и годится все, что угодно[64].

Заметим, что Интернет-преступления могут квалифицироваться по самым разным статьям УК РФ, а не только по статьям Главы

---

[62] Криминология: Учебник для вузов / Под общ. ред. д.ю.н. проф. А.И. Долговой. — 2-е изд., перераб. и доп. — М.: Изд-во НОРМА, 2003. — С. 682; Schweitzer D. Incident response: computer forensics toolkit. — Wiley, 2003. — P. 26.

[63] Кашапов Р.М., Наумов С.С. Проблемы с распространением детской порнографии в глобальной сети Интернет// Вестник Дальневосточного юридического института МВД России. — 2004. — № 2. — С. 74.

[64] Луцкер А.П. Авторское право в цифровых технологиях и СМИ: с научными комментариями к.ю.н. А.Г. Серго. — М.: КУДИЦ-ОБРАЗ, 2005. — С. 286.

28. Внедренная во все сферы деятельности Глобальная информационная сеть зачастую используется для совершения на качественно новом уровне уже известных в мире противоправных деяний, а также служит благодатной средой для формирования новых видов общественно опасных деяний. Интернет-преступления посягают на различные общественные отношения; сейчас на практике можно встретить деяния, квалифицируемые практически по любой статье УК РФ, хотя совершение некоторых из них для России пока еще редкость. Рассмотрим уголовно-правовую характеристику тех или иных деяний, которые совершаются и потенциально могут совершаться посредством Интернет, используя классификацию, данную законодателем в уголовном кодексе.

Предварительно отметим, что объективная сторона большинства преступлений отличается характером причинной связи. Обязательным признаком объективной стороны материального состава преступления является причинная связь между деянием (действием или бездействием) виновного и наступившим последствием. Преступления в сфере компьютерной информации и многие Интернет-преступления можно охарактеризовать особой формой причинности — информационной причинностью[65], которая характеризуется уже не только как передача вещества и энергии, но и как передача информации от одного предмета к другому, то есть общественно опасный результат наступает не из-за переноса энергии, а из-за переноса информации[66]. Например, создатель вируса вводит в заблуждение пользователя, выдавая вредоносную программу за полезную, и тот сам заражает свой компьютер вирусом. Хотя результата не наступило бы без действий пользователя, появляется альтернативная «ветка» причинности.

Использование Интернет дает преступнику преимущества на этапе подготовки любого преступления, облегчает взаимодействие в преступных группах и предоставляет возможность найти информацию, требуемую для совершения преступления, но не каждое преступление в современном мире можно совершить посредством Интернет, то есть не каждое общественно опасное деяние можно непосредственно совершить с помощью Интернет. Это связано с

---

[65] Парфенов А.Ф. Общее учение об объективной стороне преступления: дис. ... канд. юрид. наук: 12.00.08. — СПб., 2006. — С. 91.

[66] Кудрявцев В.Н. Причинность в криминологии. — М., 1968. — С. 8, 89.

тем, что в некоторых областях, например, в избирательных процессах, Интернет еще не используется, либо используется несущественно.

В свою очередь, есть составы УК РФ, в которых Интернет может выступать как средство и способ совершения преступления, и в некоторых случаях существуют зафиксированные в судебной практике и СМИ примеры. Заметим, что Интернет может использоваться на этапе приготовления практически к любому преступлению, поэтому мы выделяем только те составы, где Глобальная сеть может быть использована для совершения непосредственно общественно опасного деяния. Представляется, что анализ ряда составов преступлений с позиции использования при их совершении Интернет позволяет получить уголовно-правовую оценку угроз, исходящих от Глобальной сети и предложить соответствующие меры профилактики и противодействия.

Преступления против жизни и здоровья (Глава 16 УК РФ). Первым зафиксированным фактом убийства, совершенным посредством Интернет, был случай, произошедший в феврале 1998 г. в США. Тяжело раненный свидетель преступления был спрятан в закрытом госпитале на территории военной базы. Преступники через Интернет изменили режимы работы кардиостимулятора и аппарата вентиляции легких, что привело к смерти[67].

В то время, когда Интернет используется все чаще в жизненно важных системах, возможностей для совершения преступлений становится все больше. Пока по Интернет нельзя стать исполнителем разве что заражения ВИЧ-инфекцией или венерической болезнью (ст. ст. 121, 122 УК РФ), хотя потенциально такая возможность существует, так как Интернет используется в медицинских и эпидемиологических учреждениях. Даже там, где исполнителем преступления посредством Интернет стать не получается, Глобальная сеть предоставляет широкие возможности для организации, пособничества и подстрекательства в преступлении практически любой статьи Особенной части УК РФ. По нашему мнению, способы причинения вреда и лишения жизни посредством Интернет можно разделить следующим образом по типу воздействия на систему ЭВМ:

---

[67] Кесареева Т.П. Криминологическая характеристика и предупреждение преступности в Российском сегменте сети Интернет : дис. ... канд. юрид. наук: 12.00.08. — М., 2002. — С. 20.

• временное нарушение работы системы ЭВМ или ее полная остановка, например, остановка работы системы обеспечения жизнедеятельности или поддержания здоровья;

• изменение характеристик и порядка работы системы ЭВМ, например, изменение параметров работы бортового компьютера автомобиля;

• запуск программ ЭВМ, который угрожает жизни или здоровью людей, например, запуск электроцепи во время электромонтажных работ.

Интернет позволяет воздействовать как на целый комплекс ЭВМ, так и на отдельные его составляющие, — например, на отдельный компьютер или конкретно на программу жизнеобеспечения на нем. Преступник может создать компьютерный «вирус», который выведет из строя всю систему энергоснабжения больницы, что приведет к остановке компьютера, контролирующего кардиостимулятор, и других ЭВМ, а может «заразить» вредоносной программой только один компьютер, к которому подключен кардиостимулятор, или программу на нем.

Заметим, что Интернет в данном случае дает преступнику возможность охватить неограниченно большой круг лиц по всему миру; кроме того, использование Глобальной сети придает преступнику чувство уверенности в своей безнаказанности и создает трудности в его привлечении к уголовной ответственности. Хотя о широкой распространенности преступлений против жизни и здоровья посредством Интернет говорить еще рано.

Преступления против свободы, чести и достоинства личности (Глава 17 УК РФ). Анонимность, безграничные возможности в распространении информации любых видов, широкая аудитория делают Интернет незаменимым средством в доставке информации массам. Отсутствие фактического контроля со стороны государства и контроля отраслевыми структурами Интернет-услуг делает возможным распространение информации самого разного рода, включая общественно опасную, это могут быть оскорбительные, посягающие на честь и достоинство клеветнические измышления, заведомо ложные сведения.

Объективную сторону ст. 129 «Клевета» образует распространение сведений в любой форме: устно, письменно или в виде изображения. Интернет позволяет распространять информацию любого вида из перечисленных. Кроме указанных, в Глобальной сети

могут публиковаться сфабрикованные клеветнические видео- и аудиоматериалы.

Например, Российская газета пишет, что со своего служебного компьютера 30-летний житель Красноярска отправил клеветническое послание не куда-нибудь, а на электронную почту ГУВД. В своем сообщении он рассказал сотрудникам милиции о якобы неблаговидной и порой незаконной деятельности своего знакомого. Против него было возбуждено уголовное дело по статье 129 УК РФ (распространение заведомо ложных сведений, порочащих честь и достоинство). В ходе расследования мужчина рассказал, что он конфликтовал со знакомым и с помощью клеветнического письма хотел создать ему проблемы с правоохранительными органами. Материалы данного дела переданы в суд. Клеветнику грозит от 3 до 6 месяцев лишения свободы, а также, возможно, большой штраф за моральный ущерб[68].

Интернет предоставляет широкие возможности и для нанесения оскорбления (ст. 130 УК РФ). Оскорбительные действия могут быть совершены посредством Интернет: устно — в голосовых чатах; письменно — в виде текстовых сообщений в чатах или при помощи электронной почты; в телодвижениях — жестами в видеоконференциях; пересылкой файла — видео, музыкального или графического. В Интернет-форумах Владивостока, например, можно часто встретить, что комментаторы тех или иных сообщений оскорбительно отзываются друг о друге, сопровождая свои сообщения унижающими человеческое достоинство изображениями. Такая практика носит повсеместный характер и стала чуть ли не нормой для общепринятого Интернет-общения.

Представляется, что распространение клеветнических и оскорбительных материалов с помощью Интернет и других распространенных компьютерных сетей более общественно опасно, так как по сравнению со СМИ с определенным тиражом и аудиторией, может охватывать неограниченно большой круг лиц по всему миру, а также может быть опубликовано анонимно или от имени другого лица, порождая чувство безнаказанности и безопасности преступника и создавая трудности для расследования. Данное явле-

[68] Корзун В. Красноярца привлекут к уголовной ответственности за клевету [Электронный ресурс] // Российская газета. — Режим доступа: http://www.rg.ru/2006/12/08/kleveta.html

ние заставляет подробней рассмотреть вопрос о введении нового квалифицирующего признака — «совершение посредством глобальной компьютерной сети», так как использование возможностей Интернет увеличивает общественную опасность преступлений.

Преступления против половой неприкосновенности и половой свободы личности (Глава 18 УК РФ). В настоящее время технически невозможно совершать «Изнасилования» (ст. 131 УК РФ) или другие преступления из Главы 18 посредством Интернет. Но необходимо признать, что Глобальная сеть становится серьезным подспорьем насильникам, педофилам и другим преступникам, совершающим преступления против половой неприкосновенности. Посредством Интернет выполняются действия по приготовлению к совершению ряда половых преступлений. Например, В.А. Голубев утверждает, что каждый пятый ребенок в возрасте от 10 до 17 лет, использующий Интернет, с помощью сети получил предложения сексуального характера от взрослых пользователей. Каждому четвертому ребенку, вступившему через чаты в переписку со взрослыми пользователями, были показаны картинки и фотографии порнографического характера[69].

Схема, по которой действуют Интернет-педофилы в поисках новой жертвы, проста. Преступники входят в детские чаты[70] и там знакомятся с детьми. Немного поговорив и завоевав доверие ребенка, преступник назначает ребенку (подростку) личную встречу — предлоги могут быть любыми. Чтобы подтолкнуть «жертву» к встрече, педофил (или изготовитель детского порно) предлагает ребенку деньги или иное вознаграждение.

Зачастую такие знакомства происходят на специальных педофильских сайтах; представляется, что организация такого сайта предшествует ряду тяжких преступлений и стимулирует их совершение. Установление уголовной ответственности за организацию этих Интернет-притонов для педофилов может предотвратить более тяжкие преступления, такие как «Изнасилование» (ст. 131 УК

---

[69] Голубев В.А. Компьютерная преступность — проблемы борьбы с Интернет-педофилией и детской порнографией [Электронный ресурс] / Центр исследования компьютерной преступности. — Режим доступа: http://www.crime-research.ru/articles/golubev2106/

[70] Чат — Интернет-сайт для обмена текстовыми или голосовыми сообщениями.

РФ), «Насильственные действия сексуального характера» (ст. 132 УК РФ), «Половое сношение и иные действия сексуального характера с лицом, не достигшим шестнадцатилетнего возраста» (ст. 134 УК РФ) и другие преступления из Главы 18 УК РФ.

Преступления против конституционных прав и свобод человека и гражданина (Глава 19 УК РФ). «Нарушение неприкосновенности частной жизни» (ст. 137 УК РФ), а также «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» (ст. 138 УК РФ) вызывают особое опасение в последнее время. Цифровые технологии дают широкие преимущества для преступников в этой области. Так, в последнее время получила широкое распространение кража видеороликов, снятых на сотовый телефон, и последующее размещение этого личного видеоматериала в Интернет за деньги или бесплатно без ведома владельца. При помощи Интернет можно не только проникнуть на компьютер жертвы, но и посмотреть его электронную переписку, все личные файлы и личную информацию[71]. Благодаря интеграции многих технологий в Интернет, — например, Интернет-телефонии, Интернет-почты, становится возможным перехватить сообщения любого вида посредством Глобальной сети. Преступник, получив доступ посредством Интернет к компьютеру потерпевшего, фактически берет под контроль все коммуникации жертвы[72].

Еще больший простор Интернет создает для «Нарушения авторских и смежных прав» (ст. 146 УК РФ). Простота распространения информации на широкую аудиторию и копирования программных продуктов, электронных произведений позволяет легко нарушать права авторов. Интернет может служить как для того, чтобы незаконно добыть копию защищенного продукта, так и для того, чтобы распространить его. Единственное требование для распространения товара посредством Интернет — продукт должен быть в электронном виде, что накладывает ограничения на вид защищаемых авторским правом предметов преступления. Чаще всего посредством Интернет незаконно распространяются: компью-

---

[71] Bidwell T. Hack proofing your identity in the information age. — Syngress Publishing. Inc., 2002. — P. 3—6.

[72] См. например: Касперски К. Компьютерные вирусы изнутри и снаружи. — СПб.: Питер, 2007. — С. 282.

терные программы, видеофильмы, музыкальные произведения и тексты книг в электронном формате. В настоящее время сложно установить контроль за оборотом файлов в Интернет, поэтому большинство файлов распространяется в обход авторского вознаграждения. В случае крупного и особо крупного ущерба вступает в действие ст. 146 УК РФ. При этом состав ст. 146 ч.1 материальный, т. е. считается оконченным в момент причинения крупного ущерба автору или иному правообладателю[73].

Нарушение авторских прав посредством Интернет потенциально несет в себе большую опасность, так как пиратские копии произведения могут распространяться на неограниченный круг лиц по всему миру. Используя сеть, преступники могут распространять авторский продукт анонимно, создавая трудности в их привлечении к уголовной ответственности. Неперсонифицированный доступ придает преступнику чувство субъективной безопасности, которое увеличивает его решимость в выборе незаконного пути.

В связи с изложенным, есть предпосылки, по нашему мнению, для введения в ч. 2 ст. 137, ч. 2 ст. 138, ч. 3 ст. 146 Главы 19 УК РФ квалифицирующего признака «совершение посредством глобальной компьютерной сети».

Преступление против семьи и несовершеннолетних (Глава 20 УК РФ). Так как Интернет доступен не только взрослым, но и несовершеннолетним, создается угроза того, что при помощи Интернет подросток 14 — 17 лет или ребенок до 13 лет будет вовлечен в преступление (ст. 150 УК РФ). Объективная сторона данного преступления выражается в обязательном действии — вовлечении несовершеннолетнего в совершение преступления и в одном из альтернативных: 1) обещании, 2) обмане, 3) угрозе, кроме угрозы применения насилия, 4) действии, составляющем иной способ воздействия. Интернет позволяет найти злоумышленнику наиболее подходящего для осуществления своих целей психологически неустойчивого несовершеннолетнего; а также благодаря широким возможностям в вопросах коммуникации и фальсификации информации установить контакт с подростком и воздействовать на него. Например, опытный хакер может привлечь несовершенно-

[73] Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. А.А. Чекалин; Под ред. В.Т. Томина, В.С. Устинова, В.В. Сверчкова. — 2-е изд., исп. и доп. — М.: Юрайт-Издат, 2004. — С. 371.

летних к совершению преступления, рассказав им о механизме взлома Интернет-сайта и убедив в безнаказанности. При этом Интернет позволяет сделать это анонимно и безопасно.

Кроме этого, Интернет может служить подспорьем при вовлечении в антиобщественное поведение (ст. 151 УК РФ). Так, существуют сайты, убеждающие посетителей употреблять спиртные напитки или психоактивные вещества, при этом доступ к таким сайтам имеют и несовершеннолетние[74]. Иногда сайты, пропагандирующие алкоголизм или наркоманию, посвящены тем или иным молодежным субкультурам. Например, на сайте Минских панков (http://punksminsk.ucoz.ru/) появляются ежедневные сообщения предлагающие «побухать», а в апреле 2008 года там было размещено голосование под названием «что вы любите бухать».

Данные преступления считаются оконченными независимо от того, оказалось лицо вовлеченным или нет (ст.150, ст.151 УК РФ)[75]. То есть публикация материалов на сайте в Интернет с умыслом вовлечения несовершеннолетних в антиобщественное поведение или совершение преступления образует состав преступления, предусмотренного ст. ст. 150,151 УК РФ. Совершение таких действий посредством Интернет также позволяет достигать неограниченно большой аудитории, и попытки такого вовлечения несут больший вред. Так, например, публикация на сайте, рассказывающая о выгодности совершения преступлений и призывающая к этому, может быть прочитана любым подростком или ребенком, имеющим доступ в Интернет. Чем популярней сайт, тем больше вероятность того, что призывы дойдут до аудитории. Представляется, что использование Интернет увеличивает общественную опасность данной категории преступлений.

Преступления против собственности (Глава 21 УК РФ). Одним из самых распространенных видов преступлений современности в Интернет является Интернет-мошенничество. При этом с каждым днем появляются все новые его формы, виды и способы. Такая популярность хищения чужого имущества путем обмана или злоупотребления доверием посредством Интернет легко объясни-

---

[74] http://buxaem.narod.ru/; http://nebuhoy.narod.ru/; http://www.buhaem.net/ и др.

[75] Уголовное право. Особенная часть. Учебник / Под ред. проф. Л.Д. Гаухмана и проф. С.В. Максимова. – М.: Изд-во ЭКСМО, 2004. – С. 131,133.

ма. Интернет позволяет выдавать себя за другого человека, изменяя данные о возрасте, социальном статусе и другие идентификационные признаки, что является преимуществом при совершении мошенничества (ст. 159 УК РФ) посредством Глобальной сети. Можно, например, создать сайт в Интернет под видом юридического или частного лица и собирать средства под тем или иным предлогом путем обмана. Посредством Глобальной сети можно найти жертву, ввести в заблуждение и осуществить мошенническую финансовую операцию, то есть Интернет можно использовать практически на всех стадиях преступлений против собственности, за исключением преступлений, совершенных с применением физического насилия[76].

В качестве примера можно привести пресс-релиз с сайта по борьбе с компьютерными преступлениями департамента юстиций США. Некий Жежев, гражданин Казахстана, посредством доступа в Интернет скачал базы данных с личной информацией клиентов компании Bloomberg L.P.'s и вымогал 200000 долларов США, угрожая опубликовать эти базы в Интернет[77]. Без использования Интернет данное преступление было бы невозможно, так как вряд ли гражданин Казахстана, находящийся в другой части мира, смог получить доступ к данным Bloomberg каким-либо другим способом. Кроме трансграничных преимуществ Интернет позволил преступнику оставаться анонимным до момента его задержания в Лондоне, куда он был вызван якобы для передачи денег.

Достаточно распространенным явлением, в том числе и в Приморье, стало причинение имущественного ущерба, когда преступники бесплатно пользуются услугами Глобальной сети за счет других лиц, используя пароли, полученные у легальных пользователей путем обмана. Данные дела квалифицируют как по ст. 272 УК РФ, если имел место незаконный доступ, так и по ст. 165 УК РФ[78].

---

[76] См. например: Гончаров Д. Квалификация хищений, совершаемых с помощью компьютеров // Законность. — 2001. — № 11. — С. 32.

[77] Kazakhstan Hacker Sentenced to Four Years Prison for Breaking into Bloomberg Systems and Attempting Extortion [Электронный ресурс] / Computer Crime & Intellectual Property Section U.S. Department of Justice. — Режим доступа: http://www.cybercrime.gov/zezevSent.htm

[78] Лопатина Т.М. Противодействие преступлениям в сфере компьютерной информации // Законность. — 2006. — № 6. — С. 51.

Вследствие внедрения Интернет-технологии стало возможным умышленно уничтожать или повреждать имущество (ст. 167 УК РФ), в основном компьютерную технику, подключенную в Интернет. Так, например, с помощью Интернет можно вывести из строя не только программную оболочку, но и саму технику, которая не подлежит быстрому восстановлению, а ее ремонт потребует значительных финансовых затрат. Данные преступления попадают под квалификацию по ст. 167 УК РФ.

Кроме прямого ущерба в виде стоимости устройства, также может быть нанесен ущерб из-за выхода устройства в структуре компьютерной сети, в связи с потерей одного из важных передающих звеньев (что снижает ценность отдельной сети), или из-за уничтожения информации, содержащейся на устройстве, и, как следствие, другие трудности: срыв поставки товара, невыполнение обязательств и т.д. Использование Интернет позволяет преступникам, совершающим преступления против собственности, охватывать огромный круг лиц. Например, после урагана Катрина в США был создан сайт, который якобы собирал денежные средства для пострадавших; с помощью него преступники завладели 80 млн долларов США, а в результате так и не были задержаны.

Использование Интернет в совершении преступлений данной группы также увеличивает их общественную опасность. Так как жертвами, например, Интернет-мошенничества может стать огромное число лиц, практически любой пользователь Интернет. К тому же Интернет создает проблемы для выявления и преследования преступников и они успевают уничтожить улики своего преступления.

Преступления в сфере экономической деятельности (Глава 22 УК РФ). Простота и дешевизна создания Интернет-сайтов (от 50 долларов США) привела к тому, что «открыть» свое дело в Интернет дешево и быстро. Это повлекло открытие в Глобальной сети многочисленных Интернет-магазинов, Интернет-услуг, Интернет-«барахолок» и т.д. Отсутствие правового контроля в Глобальной сети за подобной деятельностью привело к тому, что зачастую предпринимательская деятельность осуществляется без регистрации или без специального разрешения, без оплаты налогов и т. д. При этом нелицензированная деятельность осуществляется не только в сфере предпринимательства (ст. 171 УК РФ), но и в сфере банковской деятельности (172 УК РФ).

Благодаря появлению таких систем оборота денежных средств в Интернет, как PayPal (США), WebMoney (СНГ) и т.д., стало возможным осуществлять банковские операции (банковскую деятельность) без регистрации и без специального разрешения (лицензии), когда такое разрешение обязательно, такая деятельность составляет объективную сторону ст. 172 УК РФ[79]. В Интернет работает большое количество сайтов, занимающихся кредитными, валютными операциями без каких-либо разрешительных документов и без элементарной регистрации. Например, существуют обменные пункты в Интернет, которые позволяют перевести деньги из одной валюты в другую и даже вывезти деньги за рубеж без документов. Бесконтрольность международных и внутренних денежных потоков позволяет легко легализовать (отмыть) денежные средства, приобретенные преступным путем (ст. 173 УК РФ), не возвращать средства в иностранной валюте из-за рубежа (ст. 193 УК РФ), уклоняться от уплаты налогов (ст. ст. 198, 199 УК РФ).

Операции, совершаемые с Интернет-деньгами, происходят за секунды, зачастую не оставляя постоянных бумажных следов, а только временные электронные. Так как часто возникают трудности в установлении компьютера, с которого осуществлялась операция, а также лица, которое ее совершало, то следует сказать, что преступники могут действовать, ощущая себя безнаказанными. Этими услугами пользуются и преступники в других сферах. Так, например, распространители порнографии могут принимать деньги в системе PayPal за рубежом и свободно совершать с ними операции, оставаясь анонимными (подобная схема оплаты описана в журнале «Хакер»), и через определенные сайты можно ввезти в Россию или, наоборот, вывезти из нее средства в любой валюте мира, также абсолютно анонимно[80]. Таким образом, Интернет позволяет преступнику, совершающему преступления, квалифицируемые по статьям Главы 22 УК РФ, чувствовать себя безнаказанно, затрудняя возможность его привлечения к уголовной ответственности, и игнорировать государственные границы.

---

[79] Куликов Е.М. Незаконная банковская деятельность: уголовно-правовые и криминологические проблемы: дис. ... канд. юрид. наук: 12.00.08. — Ставрополь, 2001. — С. 46.

[80] См., например: http://exwp.com/

Преступления против общественной безопасности (Глава 24 УК РФ). В связи с тем, что Интернет проник во все сферы человеческой деятельности, стало возможным посредством Глобальной сети совершать действия, создающие опасность гибели людей, причиняющие значительный имущественный ущерб, нарушающие общественную безопасность, с целью устрашения населения, либо оказания воздействия на принятие решений органами власти. Другими словами, Интернет стал новой возможностью для совершения актов терроризма (ст. 205 УК РФ). Наибольшей опасности подвержены коммуникационные узлы. Но в связи с тем, что к Интернет подключены компьютерные системы стратегических подразделений, органов государственной власти и т.д., зачастую выбираемые террористами для атаки; теракт посредством Интернет может быть произведен против большого количества объектов.

Интернет сейчас задействован практически во всех сферах жизни, средства коммуникации, средства массовой информации, коммунальные службы, крупные производства. Вторжение террористов по Интернет может нанести огромный ущерб и при этом они останутся безнаказанными.

Глобальная сеть создает определенные преимущества для террористических организаций как для вербовки или финансирования (ст. 205[1] УК РФ), получения информации о цели, дезинформации об актах терроризма (ст. 207 УК РФ), так и собственно для совершения террористических действий. Такие качества Интернет, как глобальность и анонимность, делают его удобным инструментом международного и внутригосударственного терроризма. Так как в первую очередь Глобальная сеть — это информационная среда, Интернет может послужить средством для распространения информации, необходимой для незаконного изготовления оружия (ст. 223 УК РФ) и незаконных операций с взрывчатыми веществами и взрывными устройствами (ст. 222 УК РФ). Также посредством Интернет можно организовать либо спровоцировать массовые беспорядки (ст. 212 УК РФ).

Как и в случае с некоторыми другими статьями УК РФ, использование Интернет для совершения преступлений многократно увеличивает общественную опасность преступлений. Во-первых, применение Интернет стимулирует чувство безнаказанности и безопасности у преступника во время совершения преступлений. Во-

вторых, используя Интернет, преступник создает дополнительные трудности в расследовании и пресечении его действий. В-третьих, Глобальная сеть дает возможности для совершения преступлений против очень широкого круга лиц.

Преступления против здоровья населения и общественной нравственности (Глава 25 УК РФ). Угрожающий размах в Интернет приобрели сайты, пропагандирующие наркоманию, публикующие технологию изготовления наркотических препаратов в домашних или промышленных масштабах; распространяющие наркотические средства, психотропные вещества и их аналоги. Например, семена наркосодержащей конопли или опиумного мака можно заказать по электронной почте.

Еще более широкое распространение в Глобальной сети получил порнобизнес. Изготовление и оборот материалов с изображениями несовершеннолетних (ст. 242[1] УК РФ), а также распространение других порнографических материалов и предметов является одним из самых прибыльных видов преступной деятельности. В данном случае Интернет может выступать не только как среда для передачи информации, но также для осуществления приема платежей за незаконные услуги благодаря системам Интернет-денег (PayPal. WebMoney и др.). В настоящее время для порнобизнеса физический мир необходим только для изготовления порнографического материала, все другие операции: реклама, распространение, оплата осуществляются в сети. Также Интернет может использоваться для поиска «актеров» и организации взаимодействия преступных группировок, которые во многих случаях ведут деятельность на территории нескольких государств. Интернет существенно облегчает незаконную деятельность, связанную с порнографией. Как заметил А.Л. Осипенко, раньше детскую порнографию можно было получить с большим риском только в специальных клубах. Теперь же это можно делать анонимно посредством Интернет[81].

---

[81] Осипенко А.Л. Уголовно-правовые и иные средства противодействия обороту материалов с порнографическими изображениями несовершеннолетних в сети Интернет // Уголовное право. — 2007. — № 1. — С. 110. См. также: Рохлин В. Проблемы уголовного преследования за киберпреступления (детская порнография в Интернете) / В. Рохлин, С. Кушниренко // Законность. — № 3. — 2007. — С. 28—29.

Заметим, что порносайт в Интернет доступен для любой точки мира, при этом распространители безнравственной продукции чувствуют себя безнаказанно, так как действуют анонимно. Существуют и определенные трудности, вызванные использованием Глобальной сети, в привлечении их к уголовной ответственности. Исходя из анализа составов Главы 25 УК РФ, следует отметить, что при использовании Интернет также увеличивается общественная опасность данной категории преступлений.

Преступления в сфере компьютерной информации (Глава 28 УК РФ). Данные преступления — неотъемлемая часть преступности в Глобальной сети, так как сопутствуют практически всем запрещенным УК РФ деяниям, совершаемым в Интернет. Именно эти преступления нельзя назвать традиционными, так как их не существовало до появления отношений в сфере компьютерной информации. В отличие от других видов Интернет-преступлений, компьютерные технологии не просто облегчили выполнение данного вида деяний, а породили преступления этой категории, поэтому общественно опасные деяния данного вида, совершаемые посредством Глобальной сети, требуют особо тщательного анализа.

Повышение ценности информации в новом высокотехнологичном обществе вызвало необходимость в ее защите. Можно сказать, что неправомерный доступ (ст. 272 УК РФ) — характерное преступление нового общества. При этом появление такой технологии, как Интернет, сделало данный вид преступления более глобальным и безопасным для преступника.

Если до появления Глобальной сети необходим был непосредственный контакт с компьютерной системой, то появление Интернет позволило совершать преступления в других странах, не выходя из дома, при этом в высшей степени анонимно. Характерно, что большинство улик для установления местоположения и личности хранится в атакуемой системе. Проникая в систему, преступник не только совершает преступление, но одновременно решает проблему сокрытия следов.

Компьютерная система, ставшая «жертвой» вторжения посредством Интернет, может быть самой разнообразной: от компьютера министерства обороны какого-либо государства или ЭВМ банковской сети до персонального домашнего компьютера. Например, 20-летний хакер смог проникнуть в сеть NASA (National Aeronautics and Space Administration — Национальное аэрокосми-

ческое агентство в США) и получить доступ к файлам разрабатываемой системы управления полетами спутников[82].

В то же время незаконный доступ может представлять и меньшую общественную опасность. Например, один из студентов Владивостокских вузов получил доступ к домашнему компьютеру, чтобы украсть пароли доступа в Интернет и причинил ущерб на 89 руб. 32 коп[83].

Как и «Неправомерный доступ к информации» (ст. 272 УК РФ), «Создание, использование и распространение вредоносных программ для ЭВМ» (ст. 273 УК РФ) стало возможным только с появлением компьютеров. Создание и развитие Интернет раскрыло новые горизонты для данного вида преступлений. Вирусы (так называют определенные вредоносные программы), распространяющиеся по Интернет, смогли порождать целые эпидемии за счет того, что все компьютерные системы стали подключаться к единой всемирной сети. Подсчет количества «зараженных» систем от той или иной вредоносной программы ведется уже в миллионах. Например, модификация вируса Sobig (Sobig.F) появилась в Интернет 19 августа 2003 г. и поставила новый мировой рекорд (вскоре побитый MyDoom), заразив более 1 млн. компьютеров за 24 часа. Приблизительный ущерб: $5 — 10 млрд[84]. Вследствие глобальности и анонимности Интернет создатели большинства из самых разрушительных вирусов так и не найдены.

При этом набольшую опасность представляют те разновидности вредоносных программ, которые способны к самовоспроизводству и самораспространению[85]. Представляется, что среди таких вредоносных программ выделяются те, которые могут самораспространяться в Интернет.

---

[82] Orange County Computer Hacker Sentenced to Prison for Breaking into University Computers, NASA Systems [Электронный ресурс] / Computer Crime & Intellectual Property Section U.S. Department of Justice. — Режим доступа: http://www.cybercrime.gov/diekmanSent.htm

[83] См: Уголовное дело № 463522 / Следственный отдел при ОВД Первореченского района г. Владивостока, 2003.

[84] Десятка самых разрушительных вирусов в истории [Электронный ресурс] / 1ion.ru. 1ON Media Group. — Режим доступа: http://www.1on.ru/2006_07_19/desiat_samyh_razrushitelnyh_virusov_v_istorii.html

[85] Комментарий к Уголовному кодексу Российской Федерации. Расширенный уголовно-правовой анализ / Под общ. Ред. В.В. Мозякова. — М.: Экзамен. — С. 651.

Распространение вредоносных программ может также сопутствовать совершению других преступлений. Например, для неправомерного доступа в систему: зачастую на компьютер жертвы посылается программа, крадущая пароли или позволяющая входить в компьютерную систему без пароля. Кроме того, деструктивный заряд вирусов может быть использован для совершения терактов и ряда других преступлений. Среди них:

- вывод из строя оборудования или систем, отвечающих за жизнь и здоровье людей (ст. 105, ст. 111 УК РФ);
- распространение при помощи вируса клеветнических или оскорбительных сведений (ст. ст. 129, 130 УК РФ);
- кража персональной информации о частной жизни, а также доступ к переговорам или переписке (ст. ст. 137,138 УК РФ);
- уничтожение имущества (ст. 167 УК РФ);
- террористические акты (ст. 205 УК РФ);
- действия по выводу из строя общественно важных инфраструктур, от которых зависит экономическая безопасность и обороноспособность Российской Федерации (ст. 281 УК РФ)[86].

При этом компьютерная программа, которая самопроизвольно множится посредством Интернет, очень опасна, так как в состоянии нанести ущерб неограниченно большому кругу лиц по всему миру. Как отмечают некоторые авторы, внедрение компьютерных вирусов в сети позволяет причинить вред обществу и государству в целом[87]. Таким образом, распространение вредоносных программ *посредством Интернет* может служить дополнительным квалифицирующим признаком. Осуществляя неправомерный доступ к компьютерной информации (ст. 272 УК РФ) и распространяя вредоносные программы для ЭВМ (ст. 273 УК РФ) посредством Интернет, преступник также чувствует себя безнаказанно и создает дополнительные трудности для правосудия.

---

[86] Предложенный перечень открыт, так как создатели вредоносных программ не стоят на месте, и каждый день разрабатываются новые вирусы. Представляется, что вирусы применимы в любых Интернет-преступлениях, которые требуют вывода из строя компьютерной системы или систем, а также в преступлениях, где информация в электронном виде может быть распространена на неограниченно большой круг лиц.

[87] Лопатина Т.М. Виктимологическая профилактика компьютерных преступлений // Российская юстиция. — 2006. — № 4. — С. 53

Представляется необходимым рассмотреть возможность законодательно ввести в Главу 28 УК РФ, в ч. 2 ст. 272, ч. 2 ст. 273 УК РФ такой квалифицирующий признак, как «совершение посредством глобальной компьютерной сети».

Преступления против основ конституционного строя и безопасности государства (Глава 29 УК РФ). С ростом использования Интернет в государственных структурах становится возможным нелегально получить доступ не только к частной и корпоративной информации, но также к информации, являющейся государственной тайной, и посредством Глобальной сети совершать такие преступления, как шпионаж (ст. 276 УК РФ) или государственная измена (ст. 275 УК РФ), разглашение государственной тайны (ст. 283 УК РФ).

К Интернет подключены также многочисленные предприятия, сооружения, пути, средства сообщения, узлы связи и объекты жизнеобеспечения, от которых зависит экономическая безопасность и обороноспособность государств. В Америке, например, уже давно озабочены проблемой диверсий посредством Интернет. Опасность подвергнуться диверсии (ст. 281 УК РФ) напрямую зависит от внедрения Интернет во все сферы деятельности и, следовательно, такая опасность будет с каждым годом возрастать как в других странах мира, так и в России[88].

Из-за роста аудитории российского Интернет вызывает опасение возможность распространять посредством Интернет информацию, направленную на возбуждение ненависти или вражды на национальной либо религиозной почве, а также унижающую человеческое достоинство как отдельного человека, так и группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой-либо социальной группе (ст. 282 УК РФ). Прорасистские сайты получили в последнее время широкое распространение в русскоязычном Интернет. Так, на сайте национал-социалистического движения «Славянский союз»[89] открыто унижают людей по национальному признаку и призывают к конфронтации[90].

---

[88] Timothy Shimeall, Phil Williams, Casey Dunlevy. Countering cyber war [Электронный ресурс] / NATO Review vol. 49. — № 4. Winter 2001. — Режим доступа: http://www.nato.int/docu/review/2001/0104-04.htm

[89] http://ns-rus.cc/infowar/articles/18.shtml

[90] На этом сайте можно найти «доктрину фашизма», «18 советов белому воину» и массу других откровенно профашистских материалов.

Из всего вышесказанного можно сделать вывод о чрезвычайной распространенности и многоликости Интернет-преступности как в целом, так и в отдельных ее видах. Преступления, которые возможно совершать посредством Интернет, охватывают практически все Главы УК РФ. Особенности характеристики преступности глобальной сети не исчерпаны, и они подробно будут раскрыты в монографии. По нашему мнению, Интернет-преступность легко выделяется в отдельный вид как криминологическими характеристиками, так и уголовно-правовыми признаками. Несмотря на различие составов, по которым квалифицируются или могут квалифицироваться современные Интернет-преступления, все из подвидов преступности в Глобальной сети образуют единую систему и взаимосвязаны между собой.

В свою очередь заметим, что в ряде составов УК РФ совершение преступлений посредством Интернет увеличивает общественную опасность деяний. Это составы, предусмотренные ст. ст. 105, 111, 112, 115, 119, 129, 130, 135, 137, 138, 141, 146, 147, 150, 151, 158, 159, 163, 167, 171, 172, 173, 174, 174^1, 205, 205^1, 205^2, 215^2, 228, 228^1, 230, 242, 242^1, 272, 273, 274, 276, 280, 281, 282, 283, 298 УК РФ. Во-первых, возрастает общественная опасность лица, совершающего преступления, то есть использование компьютерной сети придает преступнику чувство безнаказанности и увеличивает его решимость в совершении преступления, так как облегчается возможность реализации задуманного деяния и сокрытия следов содеянного. Во-вторых, во многих случаях Интернет-преступление потенциально несет в себе большую общественную опасность. В-третьих, лицам, совершающим преступные деяния, — например, изготовление материалов или предметов с порнографическими изображениями несовершеннолетних (ст. 242^1 УК РФ) и другие, осуждаемые широкой общественностью, Интернет дает возможность уйти от общественного порицания и создает дополнительный спрос на нравственно опасную информацию, так как позволяет потребителям подобной продукции делать это анонимно. Выше перечисленное соответствует нескольким критериям дифференциации уголовной ответственности сразу[91]: при использовании Интернет для совер-

[91] Коробеев А.И. Уголовно-правовая политика: тенденции и перспективы / А.И. Коробеев, А.В. Усс, Ю.В. Голик. — Красноярск: Изд-во Красноярского университета, 1991. — С. 90.

шения общественно опасного деяния наблюдается как увеличение степени общественной опасности самого деяния, так и деятеля.

Об увеличении общественной опасности преступления при использовании Интернет говорят и другие авторы. Интернет позволяет действовать, не замечая границ. Характерной чертой данных преступлений является повышенная степень общественной опасности и огромный размер преступных доходов, во много раз превышающий наживу от обычных хищений[92]. *Несмотря на то, что при совершении преступного деяния посредством Интернет фактически причиненный вред может и не отличаться от вреда в преступлениях без использования сети, общественная опасность включает в себя не только объективно причиненный ущерб, но и тот ущерб, который потенциально мог быть. А при использовании Интернет непосредственно для совершения деяния вред может быть нанесен неограниченно огромному количеству пользователей по всему миру, то есть увеличивается общественная опасность.*

Следует также отметить, что большинство преступлений дестабилизируют нормальное функционирование Интернет, то есть преступник при использовании Глобальной сети для совершения деяния посягает не только на непосредственный объект преступления, но и на общественные отношения, которые возникли в ходе развития Интернет и значимость которых с каждым годом увеличивается. Общественная опасность при этом возрастает, так как зависит от значимости общественных отношений, на которые посягает преступник.

Но этого недостаточно для отнесения «использования глобальных компьютерных сетей» к отягчающему обстоятельству. Например, С.Е. Кротов отмечает, что отягчающее обстоятельство, регламентируемое общей частью УК, должно быть *типичным и характерным* для большого числа составов[93]. Большое количество составов по которым могут совершаться преступления с помощью

---

[92] Завидов Б. Сфера высоких технологий как объект преступления // Уголовное право. — № 3. — 2002. — С. 110.

[93] Кротов С.Е. Дифференциация уголовной ответственности в зависимости от категоризации преступлений, квалифицирующих признаков и обстоятельств, отягчающих наказание: дис. ... канд. юрид. наук: 12.00.08. — М., 2005. — С. 98—99.

сети Интернет говорит о типичности данного явления. Более того, оно не только типично, но и широко *распространено*. Например, большая часть порнографии (ст. 242, 242[1] УК РФ), вредоносных программ (ст. 273 УК РФ) в основном распространяются посредством Глобальной сети Интернет. Неправомерный доступ (ст. 272 УК РФ) также осуществляется преимущественно посредством сети Интернет.

Динамика роста использования Интернет для совершения преступлений говорит в пользу введения рассматриваемого отягчающего обстоятельства. Как более эффективный и безопасный для преступника способ совершения преступления посредством Интернет вытесняет другие менее эффективные средства и способы. По некоторым составам количество преступлений, совершаемых посредством Интернет, давно достигло 50% среди остальных и продолжает увеличиваться: например, распространение порнографии (ст. 242 УК РФ) или нарушение авторских и смежных прав (ст. 146 УК РФ).

Введение такого признака не создаст дополнительных трудностей и не потребует дополнительных возможностей уголовной юстиции. В большинстве уголовных дел и так устанавливают, использовался ли Интернет непосредственно для совершения преступного деяния. Это не требует дополнительных экспертиз и выемок, так как для сбора улик обязательно проводится компьютерная экспертиза и выемка компьютера, если он использовался для совершения преступления. Например, в постановлении о прекращении дела № 1-353 при описании способа совершения преступления было указано, что чужой пароль был получен посредством Интернет-доступа к системе ЭВМ потерпевшего[94]. А в уголовном деле № 1-1564 описаны даже сеансы работы посредством Интернет и подробно раскрыты неправомерные действия, совершаемые при помощи Интернет[95].

Для некоторых составов использование Интернет для совершения преступного деяния не только не редкость, но является ти-

---

[94] Уголовное дело № 705622 МВД России, следственный отдел при УВД Первореченского района г. Владивостока.

[95] Постановление о прекращении уголовного дела № 1-1564/ 2006 Петропавловск-камчатского городского суда Камчатской области от 18 декабря 2006.

пичным способом совершения преступления, что позволяет поднять вопрос о целесообразности введения квалифицирующего признака в данные составы. Заметим, что не только повышенная степень общественной опасности, но и типичность того или иного вида обстоятельства деяния является необходимым критерием для его отнесения к квалифицирующим признакам[96]. Например, А.Н. Трайнин отмечал, что лишено смысла закреплять в законе в качестве квалифицирующего признака преступления единичные обстоятельства, даже если они значительно влияют на степень общественной опасности[97].

При таком условии вопрос о приемлемости введения квалифицирующего признака «совершение преступлений посредством компьютерных сетей» уместен лишь для некоторых составов УК РФ, где Интернет не только увеличивает степень опасности преступления, но и является типичным способом совершения данного вида преступлений. К таким составам вряд ли можно отнести, например, убийство (ст. 105 УК РФ) или другие составы из Главы 16 УК РФ «Преступления против жизни и здоровья».

С другой стороны, есть ситуации, когда преступления, совершаемые посредством Интернет, просто менее выявляемые, хотя и более распространены. Например, распространение порнографии в Интернет не соответствует даже общему количеству зарегистрированных по ст. 242 УК РФ. То есть существуют составы преступлений, в которых использование Интернет является типичным, но сами эти деяния выпадают из поля зрения правоохранительных органов. Подробнее оценка распространенности тех или иных деяний рассмотрена в § 3.1., 3.2. То есть при оценке типичности использования Интернет для того или иного состава мы пользовались не только данными официальной статистики, но и результатами исследований, оценками экспертов, мнением самих Интернет-преступников.

Исходя из анализа составов преступлений УК РФ, которые возможно совершать посредством Интернет, есть основания ввести

---

[96] Кротов С.Е. Дифференциация уголовной ответственности в зависимости от категоризации преступлений, квалифицирующих признаков и обстоятельств, отягчающих наказание: дис. ... канд. юрид. наук: 12.00.08. — М., 2005. — С. 150.

[97] Трайнин А.П. Состав преступления по советскому уголовному праву. — М.: Госюриздат, 1951. — С.88.

в ст. 63 УК РФ дополнительное обстоятельство, отягчающее наказание: «совершение преступления посредством глобальной компьютерной сети». Представляем теоретическую модель статей Особенной части УК РФ, в которые с криминологической точки зрения целесообразно внести изменения в виде добавления квалифицирующего признака.

Ч. 2 ст. 129 УК РФ «*Клевета, содержащаяся ... , либо совершенная посредством глобальной компьютерной сети»;* ч. 2 ст. 130 УК РФ «*Оскорбление, содержащееся ... , либо совершенное посредством глобальной компьютерной сети»;* ч. 2 ст. 137 УК РФ «*Те же деяния, совершенные ... , либо посредством глобальной компьютерной сети»;* ч. 2 ст. 138 УК РФ «*То же деяние, совершенное ... , либо посредством глобальной компьютерной сети»;* ч. 3 ст. 146 УК РФ ввести пункт д.) следующего вида: «*д.) посредством глобальной компьютерной сети»;* ч. 2 ст. 150 УК РФ «*То же деяние, совершенное ... ,а равно посредством глобальной компьютерной сети»;* ч. 2 ст. 151 УК РФ «*То же деяние, совершенное ... , а равно посредством глобальной компьютерной сети»;* ч. 2 ст. 158 УК РФ ввести пункт д.) в следующей редакции: «*д.) посредством глобальной компьютерной сети»;* ч. 2 ст. 159 УК РФ «*Мошенничество, совершенное ... , либо посредством глобальной компьютерной сети»;* ч. 2 ст. 163 УК РФ ввести пункт д.) следующего вида: «*д.) посредством глобальной компьютерной сети»;* ч. 2 ст. 167 УК РФ «*Те же деяния, совершенные ... , а равно посредством глобальной компьютерной сети»;* ч. 2 ст. 205^1 УК РФ «*Те же деяния совершенные ... , «либо посредством глобальной компьютерной сети»;* ч. 2 ст. 230 УК РФ ввести пункт д.) в следующей редакции: «*д.) посредством глобальной компьютерной сети»;* ч. 2 ст. 242 УК РФ ввести часть 2 в следующей редакции: «*Те же деяния, совершенные посредством глобальной компьютерной сети ...»;* ч. 2 ст. 242^1 УК РФ ввести пункт г.) следующего вида: «*г.) посредством глобальной компьютерной сети»;* ч. 2 ст. 272 УК РФ *«То же деяние, совершенное ... , либо посредством глобальной компьютерной сети»;* ч. 2 ст. 273 УК РФ *«Те же деяния, повлекшие ... либо совершенные посредством глобальной компьютерной сети»;* ч. 2 ст. 280 УК РФ «*Те же деяния, совершенные ... , либо посредством глобальной компьютерной сети»*

Подводя итоги, отметим, что Интернет-преступность — это разновидность современной преступности, имеющая такие свои отличительные особенности, как глобальность, неперсонофици-

рованность, интеллектуальная природа, общедоступность, высокая латентность, быстрый рост, широкая распространенность, транснациональность, а также характеризующаяся своеобразием показателей структуры, состояния и динамики. Кроме того, использование Интернет в преступлениях, как уже отмечено, должно иметь уголовно-правовое значение, так как увеличивает общественную опасность деяния.

Глава 2. Криминологическая характеристика Интернет-преступности

2.1. Состояние, структура и динамика Интернет-преступности в России

Ключевое место в анализе преступности занимает анализ ее состояния, структуры и тенденций развития. Именно качественно-количественная характеристика преступности является отправной точкой криминологического исследования. Не зная масштаба данного вида преступлений, сложно что-либо говорить о причинах, последствиях и необходимых мерах борьбы и профилактики. По мнению многих авторов, статистика не отражает реального состояния современной преступности, но количественные характеристики могут дать представление об ее основных тенденциях в том или ином государстве (регионе) за определенный промежуток времени.

При анализе криминологических характеристик Интернет-преступности необходимо учитывать несколько факторов: во-первых, высокую латентность данных преступлений, во-вторых, то, что в Российской Федерации отдельно не ведется официальная статистика преступлений, совершаемых посредством сети, или деяний, где предметом посягательства являются какие-либо объекты Глобальной сети[98].

Даже если бы такая статистика по России была, то высока вероятность того, что в нее попадает менее организованная и опасная часть Интернет-преступности. Недостаток информационных данных заставляет проводить научные исследования, используя косвенные показатели. Так, в России ведется официальная статистика преступлений в сфере компьютерной информации (Глава 28 УК РФ), но не все общественно опасные деяния, подразумевающие уголовную ответственность по ст. ст. 272, 273, 274 УК РФ, со-

[98] Статистика ведется по компьютерным преступлениям определенных категорий, среди которых не выделяются преступления, совершенные посредством Интернет.

вершаются посредством Интернет. Неправомерный доступ (ст. 272 УК РФ) может быть осуществлен при непосредственном физическом контакте с атакуемой системой, а вредоносная программа (ст. 273 УК РФ) может распространяться при помощи дискет, компакт-дисков или других носителей.

Несмотря на то, что официальная статистика ведется по всем преступлениям (в том числе и не Интернет-преступлениям) в сфере компьютерной информации, среди них преобладают преступления, совершенные посредством Интернет. Это подтверждают некоторые региональные и общероссийские исследования. Например, в Республике Дагестан самым частым преступлением является неправомерный доступ к сети Интернет посредством чужих реквизитов (в 2003 г. — 100% от всех преступлений в сфере компьютерной информации)[99]. Следовательно, статистика по преступлениям в сфере компьютерной информации может быть использована для оценки характеристик Интернет-преступности.

Результат проведенного нами анализа уголовных дел в Приморском крае по статьям Главы 28 УК РФ также подтвердил, что преобладающим видом преступления является незаконный доступ посредством Интернет. Представляется, что количество преступлений в сфере компьютерной информации коррелирует с количеством Интернет-преступлений. Значит, статистику по преступлениям Главы 28 УК РФ вполне уместно использовать для исследования тенденций Интернет-преступности. Так, некоторые авторы уже использовали статистику по преступлениям в сфере компьютерной информации для отражения состояния данных видов преступности[100]. Мы приводим статистику преступлений в сфере компьютерной информации за последние десять лет, которая ведется Министерством внутренних дел России.

---

[99] Гаджиев М.С. Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан): дис. ... канд. юрид. наук: 12.00.08. — Махачкала, 2004. — С. 23.

[100] См: Гаджиев М.С. Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан): дис. ... канд. юрид. наук: 12.00.08. — Махачкала, 2004. — С. 21; Добровольский Д.В. Актуальные проблемы борьбы с компьютерной преступностью: дис. ... канд. юрид. наук: 12.00.08. — М., 2005. — С. 47.

Таблица 1

Сведения по России о количестве зарегистрированных преступлений в сфере компьютерной информации (Глава 28 УК РФ) за период 1997–2007 гг.

Год / Показатель	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007
Количество зарегистрир. преступлений	33	67	285	800	2072	4050	7549	8739	10214	8889	7236
Прирост в % по сравнению с предыдущим годом	-	103	325,4	180,7	159	95,5	86,2	15,9	16,9	-13	-18,6
Доля в % в зарегистрир. преступлениях	0,0013	0,003	0,01	0,027	0,07	0,07	0,27	0,3	0,29	0,23	0,2

Получается, что число зарегистрированных преступлений данной категории выросло в 309 раз с 1997 по 2005 гг. Можно отметить отсутствие роста преступлений последние 2 года. Замедление роста было предсказуемо, в 2005 г. по сравнению с 2004 г. количество уголовно запрещенных деяний в сфере компьютерной информации выросло на 16,9%, а прирост общего числа зарегистрированных преступлений составил 22,8%, соответственно уменьшилась и доля преступлений по статьям Главы 28 УК РФ в структуре всей преступности. А рост пользователей Глобальной сети в России составил около 19%. То есть согласно статистике уже в те годы количество преступлений в сфере компьютерной информации растет медленней, чем вся преступность и количество пользователей российского Интернет. В последние годы 2006 – 2007 гг. рост количества зарегистрированных преступлений остановился, и наблюдается некоторое снижение данного показателя, хотя говорить об устойчивости тенденции уменьшения числа этой категории преступлений еще рано.

Данный факт можно, конечно, объяснить и эффективностью мер противодействия и профилактики этого вида правонарушений, но есть и другие версии. Как известно, статистика не точно отражает реальное положение вещей в этой области. Во-первых, Интернет-преступность могла приобрести новые формы общественно опасных деяний, которые не охватываются статьями Гла-

вы 28. Так, например, в США самым распространенным видом преступления в сети является мошенничество на Интернет-аукционах. Представляется, что и в России этот вид преступлений достаточно распространен, но данный факт не нашел отражения в официальной статистике. Во-вторых, у любой системы, в том числе и правоохранительной, существует максимальный предел количества преступлений, которое она может обнаружить и зарегистрировать, что увеличивает латентность данного вида преступлений. Это в некоторой мере предопределяет качество официально регистрируемых в РФ преступлений по Главе 28 УК РФ. Ведь чем более ограничены возможности правоохранительных органов, тем чаще опасные и хорошо организованные Интернет-преступления остаются вне статистики. В-третьих, часто на статистику влияют «многоэпизодные» дела (150 — 200 эпизодов), которые сильно влияют на статистику в том или ином регионе. То есть 2 — 3 уголовных дела могут дать 300 — 600 зарегистрированных преступлений.

Таблица 2

Сведения по России о количестве зарегистрированных преступлений, предусмотренных ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» за период 1997—2006гг[101]

Год / Показатель	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006
Количество зарегистрир. преступлений	21	54	206	584	1637	3719	6839	7708	8322	7704
Прирост в % по сравнению с предыдущим годом	-	166,7	281	183,5	180,3	127,2	83,9	12,7	8	-
Доля среди преступлений по Главе 28 в %	63,6	80,6	72,3	73	79	91,8	90,6	88,2	81,5	-

[101] Данные за 2006 г. взяты с сайта cyberpol.ru., так как данные за другие года незначительно (1 — 5%) отличаются, то прирост и доля не указаны.

Основную долю в статистике занимают преступления, предусмотренные ст. 272 УК РФ, хотя по результатам нашего опроса 100% из опрошенных специалистов в сфере информационных технологий сообщило, что их компьютерные системы подвергались заражению компьютерными вирусами, а значит распространение вредоносных программ (ст. 273 УК РФ) также можно отнести к распространенным явлениям, однако в реалии данный вид преступлений в 4 — 6 раз реже регистрируется органами внутренних дел. Этот факт можно объяснить двумя причинами: во-первых, распространение вредоносных программ (ст. 273 УК РФ) более латентно, так как зачастую не сопряжено с прямыми материальными убытками (некоторые вредоносные программы абсолютно безобидны); во-вторых, за неправомерным доступом всегда стоит какая-то конкретная личность, которая непосредственно этот доступ и осуществляет, а в случае с распространением вредоносных программ исходного отправителя установить практически невозможно. Сложно точно оценить соотношение этих двух видов уголовно наказуемых деяний, так как цифры, приводимые компаниями по компьютерной безопасности, могут быть завышены в силу заинтересованности в привлечении интереса к этой проблеме.

Таблица 3

Сведения по России о количестве зарегистрированных преступлений, предусмотренных ст. 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ» за период 1997—2006гг[102]

Год / Показатель	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006
Количество зарегистрированных преступлений	1	12	79	172	316	323	700	1020	1890	1625
Прирост в % по сравнению с предыдущим годом	-	1100	558,3	117,7	83,7	2,2	116,7	45,7	85,3	-
Доля среди преступлений в сфере компьютерной информации в %	3,03	17,9	27,7	21,5	15,3	8	9,3	11,7	18,5	-

[102] Данные за 2006 г. взяты с сайта cyberpol.ru., так как данные за другие года незначительно (1 — 5%) отличаются, то прирост и доля не указаны.

Из анализа данных статистики зарегистрированных деяний, квалифицируемых по ст. 273 УК РФ, представляется, что наибольший удельный вес в структуре преступлений в сфере компьютерной информации занимал в 1999 г. данный вид деяний. Несмотря на то, что до 2003 г. темпы роста количества распространений вирусов были ниже и доля данного вида уменьшилась, в последние годы можно наблюдать более стремительное увеличение количества деяний.

Даже если взять среднее увеличение за последние три года (2003 — 2005), — оно возросло на 82,6% в год, то при таком росте доля данного вида преступлений в структуре преступлений в сфере компьютерной информации достигнет (при росте около 16%, который наблюдается в последние годы) уровня 1999 г., а абсолютный показатель будет равняться 3515 преступлениям. Даже сейчас, когда мы наблюдаем спад регистрируемых преступлений Главы 28 УК РФ, количество преступлений по ст. 273 УК РФ уменьшается медленней количества преступлений по ст .272 УК РФ. При этом с 1999 г. по 2005 г. произошел 45-кратный рост количества зарегистрированных преступлений по данной статье.

Представляется, что, несмотря на уменьшение количества зарегистрированных преступлений, реальная доля данного вида деяний еще вырастет, так как особых мер по борьбе с распространением вредоносных программ государством не предпринимается. Кроме этого, согласно нашему исследованию 100% респондентов использует какие-либо нелицензионные компьютерные программы (то есть в России в настоящее время нет пользователей, использующих исключительно лицензионное программное обеспечение), в том числе программы, ограждающие от вредоносных программ, которые в силу своей технической отсталости защищают только от старых вирусов, потерявших свою опасность.

Необходимо заметить, что хотя данные и касаются всех преступлений по ст. 273 УК РФ, а не только преступлений, совершенных при помощи Интернет, официальная статистика также как и в случае «Неправомерного доступа» (ст. 272 УК РФ) может использоваться при исследовании данного вида деяний в силу того, что удельный вес распространения вредоносных программ посредством Глобальной сети среди преступлений по ст. 273 УК РФ очень высок (более 2/3 от всех). Например, М.М. Менжега в ходе исследований источников инфицирования ЭВМ получил следующие

данные: Интернет — 34%; электронная почта — 31%; компакт-диски с программным обеспечением — 5%; иной источник — 2%; не известно — 28%[103].

То есть 65% приходится на заражение посредством Глобальной сети (электронная почта тоже Интернет-технология). Кроме этого возникает предположение, что в неустановленных случаях инфицирование вредоносными программами также происходило посредством Интернет. Следовательно использование данных о всех преступлениях по ст. 273 УК РФ для исследования преступлений, совершенных посредством Интернет, по той же статье вполне корректно.

Таблица 4

Данные по округам РФ о количестве зарегистрированных преступлений по статьям Главы 28 УК РФ за период 1997–2006 гг.

Если рассматривать территориальное распределение преступности в сфере компьютерной информации, то лидером здесь будет не Центральный федеральный округ, несмотря на то, что в нем располагается наибольшее количество пользователей Интернет. Первые два федеральных округа с наибольшим числом преступлений, квалифицируемых по статьям Главы 28 УК РФ, — это Северо-Западный и Приволжский. Представляется, что это можно

[103] Менжега М.М. Криминалистические проблемы расследования создания, использования и распространения вредоносных программ для ЭВМ: дис. ... канд. юрид. наук: 12.00.09. — Саратов, 2005. — С. 82–83.

объяснить различиями в социальном уровне и в уровне развития компьютерных технологий. Центральный регион превосходит другие по степени компьютеризации и количеству пользователей Интернет, поэтому доступ в Интернет и другие услуги в сфере информационных технологий там наиболее дешевы. Кроме того, в Центральном федеральном округе наилучший уровень жизни и больше возможностей легального заработка для профессионалов в компьютерных технологиях, большая часть компаний в сфере Информационных технологий располагаются именно там. Немаловажным фактором является и то, что там большее количество специалистов компьютерной безопасности. В то же время лидеры по количеству преступлений в сфере компьютерной информации — Приволжский и Северо-Западный федеральные округа хотя и имеют развитую компьютерную инфраструктуру, но уровень жизни в них значительно ниже, а также меньше возможностей для легального заработка в сфере Информационных технологий.

Таблица 5

Регионы-лидеры по количеству совершенных преступлений в сфере компьютерной информации (ст. ст. 272–274 УК РФ) за 2003–2006 гг.

Год	2003		2004		2005		2006	
Регион	Кол-во	% от	Кол-во	% от	Кол-во	% от	Кол-во	% от
1	2	3	4	5	6	7	8	9
По России	7549	100	8739	100	10214	100	8889	100
г. Москва	199	2,6	287	3,3	537	5,3	827	9,3
Нижегородская область	374	4,95	656	7,5	159	1,6	160	1,8
Калужская область	188	2,5	419	4,8	678	6,63	134	1,5
Республика Коми	946	12,5	497	5,7	2284	22,4	2289	25,8
Смоленская область	264	3,5	521	5,96	126	1,2	319	3,6
Калининградская область	579	7,7	446	5,1	24	0,2	25	0,3
Пермский край	273	3,6	552	6,3	409	4	622	7
Алтайский край	242	3,2	925	10,6	323	3,2	488	5,5
Камчатская область	691	9,2	216	2,5	328	3,2	335	3,8
Сумма по регионам	3756	49,75	4519	51,7	4868	47,7	5199	58,5

Анализ данных, приведенных в Таблице, показывает, что в ряде федеральных округов есть наиболее проблемные субъекты, на которые приходится более 50% всей преступности в сфере компь-

ютерной информации. При этом в последние три года лидирующий субъект сменился: если с 1998 по 2001 гг. лидером была Нижегородская область, то в последние годы — это Республика Коми, где в 2005 г. совершено более 22% всех преступлений по России. Что характерно, население Республики Коми в 3,5 раза меньше, чем население Нижегородской области, и в 10 раз меньше, чем население Москвы. Коэффициент количества преступлений на 100 тыс. населения в Республике Коми в 2005 г. составлял 224,2 (в 2006 г. — 224,7), а в г. Москва — всего 5,17[104] (в 2006 г. — 7,96). У Нижегородской области, демонстрировавшей самое большое количество преступлений в сфере компьютерной информации до 2001 г., коэффициент всего лишь 4,5, при этом средний показатель в 2005 г. по России составлял в сфере компьютерной информации 7,03 преступлений на 100 тыс. населения (6,12 — 2006 г.)[105].

В Дальневосточном федеральном округе выделяется Камчатская область с уровнем 91,4 преступлений на 100 тыс. населения в 2005 г. (в 2006 г. — 93,4). В настоящее время можно говорить о смещении преступности в сфере компьютерной информации из центральных и наиболее густонаселенных регионов к периферии России. По абсолютному показателю пока лидируют наиболее густонаселенные регионы (г. Москва, Нижегородская область и т.д.), но наибольшую криминализированность демонстрируют регионы с малой плотностью населения и достаточно дорогими Интернет-услугами.

Заметим, что во многих регионах ДФО показатель криминализированности выше, чем в среднем по России. При этом Камчатская область в 2003 г. была лидером по количеству преступлений на 100 тыс. населения. Таким образом, если еще в 2001 г. можно было утверждать, что наиболее криминализированными районами в области преступлений в сфере компьютерной информации считались Москва, Нижний Новгород и Санкт-Петербург[106], то в настоящее время самый высокий коэффициент преступности в сфере компь-

---

[104] Данные по количеству населения брались из результатов переписи 2002 г., см. ссылку: http://www.perepis2002.ru/ct/grf_map.htm

[105] За количество населения принято число 145,2 млн человек, согласно переписи 2002 г.

[106] Кесареева Т.П. Криминологическая характеристика и предупреждение преступности в российском сегменте сети Интернет: дис. ... канд. юрид. наук: 12.00.08. — М., 2002. — С. 65—66.

ютерной информации демонстрируют удаленные от Центра России области, например, Республика Коми и Камчатская область.

Таблица 6

Абсолютное и относительное (на 100 тыс. населения) число преступлений в сфере компьютерной информации в регионах ДФО за 2003–2006 гг.

Год	2003		2004		2005		2006	
Регион	Кол-во	На 100 тыс. насел.	Кол-во	На 100 тыс. насел.	Кол-во	На 100 тыс. насел.	Кол-во	На 100 тыс. насел.
По России	7549	5,2	8739	6,02	10214	7,03	8889	6,12
По ДФО	814	12,16	474	7,08	707	10,56	571	8,5
Республика Саха (Якутия)	6	0,63	16	1,69	24	2,53	33	3,48
Приморский край	77	3,71	168	8,11	41	1,98	52	2,51
Хабаровский край	24	1,67	58	4,04	295	20,54	145	10,09
Амурская область	6	0,66	9	0,99	9	0,99	1	0,1
Камчатская область (без а/о)	691	192,6	216	60,2	328	91,4	335	93,37
Корякский АО	0	0	0	0	0	0	0	0
Магаданская область	1	0,55	5	2,74	10	5,47	0	0
Сахалинская область	0	0	1	0,18	0	0	2	0,36
Еврейская авт. обл.	9	4,71	1	0,52	0	0	3	1,57
Чукотский АО	0	0	0	0	0	0	0	0

Одной из причин, объясняющих изменение характеристики показателей преступлений данной категории и низкий коэффициент в областях Центральной России по сравнению с другими, является реструктуризация компьютерной преступности в Центральных регионах. К тому же иногда всплеск регистрируемых преступлений обусловлен двумя тремя многоэпизодными делами. Хотя и нет официальных данных, однако на многих хакерских порталах и в печатных изданиях можно встретить утверждения о том, что мегаполисы России давно стали лидерами в таких видах незаконной Интернет-деятельности, как распространение порнографии, нелегальное распространение программного обеспечения и экономические махинации, которые гораздо доходней «банальной уголовщины» вроде неправомерного доступа или распространения вирусов. Нельзя, правда, опираться только на официальную статистику в силу высокой латентности как всей Интернет-преступности, так и отдельных ее видов.

По нашему мнению, Центральные регионы перешли на более латентные виды Интернет-преступлений. Это подтверждают и опубликованные интервью в компьютерных и бизнес-журналах. Так, большинство российских производителей и распространителей порнопродукции предпочитают в качестве места жительства и преступной деятельности Москву[107]. Более того, структура Интернет-преступности в той или иной стране или регионе отражает уровень развития данного вида противоправной деятельности.

Представляется, что и другие регионы в результате становления и развития в них Интернет-преступности должны перейти на этап роста доли Интернет-преступлений, требующих большей организованности. Это подтверждают данные по преступлениям в сфере высоких технологий в Приморском крае.

Таблица 7

Сведения о преступлениях, совершенных в сфере высоких технологий[108] за период 2003–2007 гг. по Приморскому краю

Год / Виды преступлений	2003	2004	2005	2006	2007
Неправомерный доступ к компьютерной информации ст. 272	74	153	23	45	441
Создание, использование и распространение вредоносных программ, ст. 273	5	17	21	7	2
Нарушение правил эксплуатации ЭВМ, ст. 274	0	0	0	0	0
Нарушение авторских и смежных прав, ст. 146	2	2	39	53	73
Мошенничество, ст. 159	0	0	3	2	28
Причинение имущественного ущерба путем обмана, ст. 165	5	0	0	0	3
Незаконное распространение порнографии, ст. 242	0	0	24	3	2

[107] См: Александр Кондратьев. Порно, спам и пиратская музыка: кто и как зарабатывает на них в Интернете // Forbes. – 2006. – № 3 (март). – С. 47–54.; Вершина порнобизнеса // Хакер. – 2004. – № 6 (66) июнь. – С. 52–55.

[108] Дословно отчет так и назывался: «Отчет о преступлениях, совершенных в сфере выскоих технологий» УВД Приморского края.

Согласно предоставленным официальным данным, общее количество преступлений по статьям Главы 28 УК РФ сначала уменьшилось после 2004 года (в 2006 г. — зарегистрировано 52 преступления по ст. ст. 272, 273, 274 УК РФ), зато появились преступления в сфере высоких технологий по ст. 159 УК РФ «Мошенничество»; по ст. 146 УК РФ «Нарушение авторских и смежных прав». В 2007 г. согласно официальной статистике регистрируется всплеск преступлений по ст. 272 УК РФ в Приморском крае. Однако анализ материалов уголовных дел показал, что такая цифра обусловлена всего двумя многоэпизодными делами (№ 798025 — 138 эпизодов, № 56625 — 154). По ст. 242 УК РФ «Распространение порнографии» стали регистрироваться первые преступления. Нелегальный порнобизнес в настоящее время является одним из самых выгодных незаконных видов деятельности в сети, при этом риск быть пойманным — минимален. Рост преступлений в сфере нарушения авторских и смежных прав с помощью высоких технологий связан скорее не с ростом данного вида нелегальной деятельности, а с более внимательным отношением правоохранительных органов к этой проблеме.

Таблица 8

Количество зарегистрированных и расследованных нарушений авторских и смежных прав, совершенных с использованием компьютерных и телекоммуникационных технологий (ст. 146 УК РФ)[109]

Год / Показатель	2001	2002	2003	2004	2005	2006
Количество зарегистрированных преступлений	158	205	249	528	794	1726
Прирост в % по сравнению с предыдущим годом	-	23	17,7	53	36,7	54

Как и в случае с распространением порнографии, наблюдается их быстрый рост, который связан с тем, что правоохранитель-

[109] Данные взяты с сайта cyberpol.ru

ные органы обратили свое внимание на эту проблему. Представляется, что динамика криминологического показателя также не отражает реального роста количества преступлений в сфере авторских и смежных прав.

Скорее это связано и с тем, что в России появились крупные компании производители программного обеспечения (например, 1С), а также активно действуют представительства зарубежных корпораций (особенно Microsoft), которые борются с пиратами, заставляя правоохранительные органы обращать на них внимание. Компании противодействуют распространению своих продуктов в Интернет, используя помощь правоохранительных органов.

Своего пика компьютерное «пиратство» достигло уже давно, так как более 90% продаваемых дисков произведено без соблюдения авторских и смежных прав. Также можно ожидать дальнейшего роста регистрируемых мошенничеств. Так как в США этот вид преступной деятельности в Интернет давно вышел на одно из первых мест по доходности и распространенности, подобного можно ожидать и в России в ходе дальнейшего развития отечественной Интернет-преступности. Количество регистрируемых мошенничеств, совершенных в Интернет, уже растет быстрее преступлений, квалифицируемых по статьям, входящим в состав Главы 28 УК РФ. Так, в последние годы регистрируемый рост этих общественно опасных деяний составляет 1,5 раза за год[110], тогда как количество преступлений в сфере компьютерной информации не растет и даже уменьшается.

Представляется, что рост доли более сложных и высоко организованных преступлений в структуре преступности в Интернет приведет к увеличению латентности данного вида общественного деяния; такие преступления более сложны для выявления, пресечения и привлечения к уголовной ответственности. Кроме этого для совершения преступлений по ст. 146 «Нарушение авторских и смежных прав», ст. 242 «Распространение порнографии» необходим целый ряд согласованных друг с другом противоправных действий, что приводит к появлению устойчивых организованных групп, специализирующихся на данных видах преступлений. Поэтому неизбежен рост количества Интернет-преступлений, совер-

[110] Илюшин Д.А. Возбуждение дел по «сетевым» преступлениям // Российская юстиция. — 2007. — № 2. — С. 55.

шенных группой лиц, группой лиц по предварительному сговору, организованной группой или преступным сообществом.

Чтобы не быть голословными, приведем данные (взятые с сайта cyberpol.ru) о зарегистрированных и расследованных незаконных распространениях порнографии, совершенных с использованием компьютерных и телекоммуникационных технологий.

Таблица 9

Количество зарегистрированных и расследованных незаконных распространений порнографии, совершенных с использованием компьютерных и телекоммуникационных технологий (ст. 242 УК РФ)

Показатель \ Год	2001	2002	2003	2004	2005	2006
Количество зарегистрированных преступлений	18	52	123	335	539	1141
Прирост в % по сравнению с предыдущим годом		188,9	137	172	60,9	112

Растет также и количество зарегистрированных случаев распространения порнографических материалов с изображением несовершеннолетних, совершенных с использованием компьютерных и телекоммуникационных технологий (ст. 242[1] УК РФ). Если еще в 2004 г. это было всего 13 преступлений, то в 2006 г. 252. Динамика просто угрожающая: не менее 100% роста в год. Представляется, что в дальнейшем еще несколько лет криминологи будут наблюдать такой бурный рост количества преступлений по ст.ст. 242, 242[1], и затем рост остановится. Распространение порнографии (особенно в Интернет) зачастую достаточно сложное для выявления и расследования преступление, и ресурсы правоохранительных органов быстро исчерпаются. Динамика роста вряд ли отражает актуальное положение вещей, т.е. можно не беспокоиться, что реальное количество данного вида преступлений удваивается каждый год, но вызывает беспокойство высокая латентность данного явления, связанная во многом с возможностями правоохранительных органов.

О размерах компьютерной преступности можно судить и по косвенным признакам, — например, по оценке не самой преступ-

ности, а численных характеристик деятельности, связанной с данным видом уголовно запрещенных деяний.

Большинство компьютерных преступников применяет чужие программные продукты, созданные посторонними людьми, и стандартные шаблоны совершения преступлений. По данным специалистов, в 2003 г. существовало около 30 тысяч сайтов, которые ориентированы на взлом и обучение приемам незаконного доступа[111].

Существует возможность получить информацию о популярности того или иного понятия, слова или выражения в Интернет с помощью поисковых систем (Yandex.ru. Rambler.ru, Google.ru). К сожалению, отследить состояние и динамику количества сайтов в Интернет с негативным содержанием на сайтах поиска представляется невозможным из-за размеров Глобальной сети и изменяющихся возможностей самих поисковых систем. Например, запрос при не изменившемся состоянии сети в том же «поисковике» в разное время может дать разные результаты, так как ядро поисковой системы и алгоритмы поиска непрерывно изменяются в целях совершенствования ее эффективности. Несмотря на это, поисковые сайты дают возможность получить единовременный срез ресурсов с преступной информацией. Хотя количество сайтов и методы поиска в поисковых системах непрерывно меняются, анализ результатов запросов к поисковым сайтам позволяет оценить соотношение количества Интернет-страниц той или иной тематики, а также позволяет выявить популярность и распространенность интересующей темы в сети Интернет.

Суть работы поисковой системы — найти все страницы, на которых встречается ключевое слово, при этом найденные страницы располагаются в порядке соответствия запрошенному слову. Разработчики поисковых систем предлагают новые пути ответа на вопрос: «какая страница больше соответствует ключевому слову». Задачей поисковых систем является нахождение ответа на вопрос, как найти страницу, которая наиболее авторитетна и больше других дает информации по запросу пользователя и предоставляет ее удобнее и точнее, то есть целью является приближение к

[111] Более 30 тысяч сайтов обучают компьютерному взлому [Электронный ресурс] / CNEWS.ru. — Режим доступа: http://www.cnews.ru/reviews/articles/index.shtml — 2003/04/14/143141

тому выбору «лучшей страницы», который сделал бы эксперт в данной области. Для этого используются как некоторые экспертные предположения (например, чем ближе ключевое слово к заглавию, тем страница больше соответствует), и количественные оценки (например, сколько ключевых слов найдено на странице), так и системы искусственного интеллекта. При этом современные поисковые службы довольно успешно отличают нужные страницы от страниц, где специально размещены популярные ключевые слова с целью привлечения пользователей.

Поисковые системы выдают ссылки (гиперссылки) на документы согласно их релевантности (англ. Relevant — значимый, существенный, относящийся к делу). То есть первыми в списке найденных выдаются ссылки на самые релевантные, соответствующие условиям поиска и с наименьшим подозрением на то, что это искомое слово просто размещено для привлечения пользователей, а не в составе содержательного текста. Представляется, что нет смысла в анализе ссылок дальше 100-й, так как данные ссылки мало соответствуют условиям поиска и редко посещаются пользователями поисковых систем. В свою очередь, анализ содержания документов или Интернет-страниц, на которые указывают первые найденные 100 ссылок, позволяет говорить о распространенности той или иной информации в Интернет, а также простоте поиска данной информации в сети, то есть легко ли будет пользователю (в том числе преступнику) поисковой системы найти данную информацию.

Заметим, что анализ ссылок поисковых систем в российской криминологии используется впервые. Этот метод пока нельзя рассматривать как основной, а только как альтернативный, помогающий в ситуации, когда официальные источники сильно искажают характеристики реальной структуры, состояния и динамики исследуемого вида преступности.

Первоочередной задачей исследования с помощью поисковых систем являлся анализ информации, содержащей характеристику преступлений, способы, приемы, методы и условия, способствующие совершению деяний, предусмотренных в Главе 28 УК РФ, так как общественно опасные деяния данной главы сопутствуют практически любому Интернет-преступлению.

Для того чтобы определить, насколько легко найти информацию по компьютерному взлому, нами были проанализированы

результаты 3 запросов к популярным поисковым системам (Google.ru, Rambler.ru, Yandex.ru): «как взломать сайт», «как взломать программу», «как взломать компьютер». Для установления достоверности того, что действительно ли страницы, найденные поисковыми машинами, содержат советы по взлому, были проанализированы первые 100 ссылок, выданных поисковыми системами 9—13 октября 2006 г., и повторили наши исследования 19—22 февраля 2007 г., чтобы проследить динамику изменения ситуации. То есть осуществлялся переход по первым 100 ссылкам, выданным поисковыми машинами, и анализировалось содержание страницы (так называемый контент-анализ), на которую указывала ссылка.

Таблица 10

Данные, полученные в результате запроса, «как взломать сайт» (по состоянию на октябрь 2006 г.)

Поисковая система	Количество найденных страниц/ Количество найденных сайтов	Количество подобных запросов за месяц	Найденные страницы, в которых содержались реальные советы по взлому в %	Найденные страницы, предлагающие средства для взлома %	Реклама сайтов с советами и средствами взлома %
Yandex.ru	264 641/ не менее 1 745	«взломать» — 39 445, «сайт» — 2 670 079	20	8	51
Rambler.ru	501 314/ 24 561	-	24	7	18
Google.ru	577 000/ -		28	16	33

Результатом запроса к поисковому серверу являются ссылки на сайты, которые больше всего подходят ключевым словам, в нашем случае «как взломать сайт». Нами было установлено, что более чем 20% сайтов из первой сотни, найденных поисковыми системами в результате запроса, содержат советы по взлому, следуя которым, как заверили компьютерные специалисты, действительно можно взломать сайт или компьютерную систему. От 7 до 16% ссылок приводили на Интернет-сайты, с которых можно скачать компьютерные программы, необходимые для неправомерного до-

ступа. К тому же большое количество ссылок (Yandex.ru — 51%, Rambler.ru — 18%, Google.ru — 33%) указывало на Интернет-порталы с рекламой сайтов, на которых были советы или средства для взлома.

Таблица 11

Данные, полученные в результате запроса, «как взломать программу» (по состоянию на октябрь 2006 г.)

Поисковая система	Количество найденных страниц/ Количество найденных сайтов	Количество подобных запросов за месяц	Найденные страницы, в которых содержались реальные советы по взлому в %	Найденные страницы, предлагающие средства для взлома %	Реклама сайтов с советами средствам и взлома %
Yandex.ru	108 167/ не менее 905	«взломать» – 39 445, «программу» – 1 650 397	31	11	34
Rambler.ru	193 972/ 19 480		32	11	27
Google.ru	454 000/-		31	34	17

В результате запроса к поисковым системам, «как взломать программу», было еще легче найти советы или средства взлома. Более чем 30% сайтов из первой сотни, найденных поисковым порталом в результате запроса, содержали советы по взлому компьютерных программ. От 11 до 34% ссылок указывали на Интернет-сайты, с которых можно скачать компьютерные программы, необходимые для взлома лицензионного программного обеспечения и неправомерного доступа. К тому же значительная часть ссылок (Yandex.ru — 34%, Rambler.ru — 27%, Google.ru — 17%) приводила на Интернет-порталы с рекламой сайтов, на которых были даны советы или предоставлены средства для взлома.

В результате запроса к поисковым системам, «как взломать программу», было гораздо труднее найти советы или средства взлома. Более чем 12% сайтов из первой сотни, найденных поисковым порталом в результате запроса, содержат советы по взлому компьютерных систем. Всего от 3 до 16% ссылок были на Интернет-сайты, с которых можно скачать компьютерные программы, не-

обходимые для компьютерного взлома. Меньше было ссылок (Yandex.ru — 26%, Rambler.ru — 17%, Google.ru — 27%), приводящих на Интернет-порталы с рекламой сайтов, на которых есть советы или приведены средства для взлома. Причиной столь малых процентов, по объяснению специалистов в области компьютерных технологий, стало редкое использование словосочетания «взлом компьютера», по сравнению с остальными словосочетаниями в среде профессионалов-компьютерщиков.

Таблица 12

Данные, полученные в результате запроса, «как взломать компьютер» (по состоянию на октябрь 2006 г.)

Поисковая система	Количество найденных страниц/ Количество найденных сайтов	Количество подобных запросов за месяц	Найденные страницы, в которых содержались реальные советы по взлому в %	Найденные страницы, предлагающие средства для взлома %	Реклама сайтов с советами средствам и взлома %
Yandex.ru	44 190/ не менее 1 302		15	8	26
Rambler.ru	160 391/ 16 410	«взломать» — 39 445, «компьютер» — 404 711	12	3	17
Google.ru	297 000/-		28	16	27

Представляется, что достаточно легко найти советы и средства взлома в Глобальной сети. Наше исследование подтверждает, что для любого компьютерного профессионала с помощью запроса в Интернет к поисковому сайту будет просто найти механизм взлома той или иной системы, а также получить необходимые для этого компьютерные программы. Кроме этого большое количество ссылок, найденных по данному запросу, свидетельствует о широкой распространенности данного явления в сети Интернет и, по крайней мере, говорит о большом количестве пользователей Интернет, которые интеллектуально и технически способны осуществить взлом.

Особенно широкое распространение получил взлом программ так называемый «crack», то есть модификация пиратской версии программы, для того, чтобы она могла использоваться как лицен-

зионная. Данный вид деятельности лишь в некоторых случаях попадает под уголовную ответственность и поэтому, по нашему мнению, так широко распространено в России компьютерное пиратство[112].

Следующими вопросами, которые мы поставили, были: легко ли научиться создавать вирус и пользоваться уже созданными; насколько сложно найти вирус. Термин «вредоносная программа», по мнению компьютерных специалистов, практически не употребляется; наиболее часто используется слово «вирус», обозначающее как один из подвидов вредоносных программ, так и все вредоносные программы в целом. Поэтому запросом, который мы проанализировали с целью узнать, насколько распространена информация по созданию вредоносных программ, был «как создать вирус».

Таблица 13

Данные, полученные в результате запроса, «как создать вирус» (по состоянию на октябрь 2006 г.)

Поисковая система	Количество найденных страниц/ Количество найденных сайтов	Количество подобных запросов за месяц	Найденные страницы, в которых содержались реальные советы по созданию вируса %	Найденные страницы, предлагающие средства для создания вирусов и сами вирусы %	Реклама сайтов с советами средствам %
Yandex.ru	48 004/ не менее 1 469	«создать» — 95 315, «вирус» — 68 503	12	5	42
Rambler.ru	490 076/ 24 893		28	11	12
Google.ru	2 640 000/ -		19	11	15

Представляется, что информация о том, как создать вирус, достаточно широко распространена в русскоязычном Интернет

[112] Есть вид модификации, который не является ни неправомерным доступом ст. 272 УК РФ, так как пользователь в большинстве случаев совершает взлом на своей системе, ни распространением вредоносных программ ст. 273 УК РФ, так как для взлома, за некоторым исключением, используются стандартные программистские средства.

(Yandex.ru — 12%, Rambler.ru — 28%, Google.ru — 19%). Кроме этого вызывает определенное опасение, что кроме информации можно найти уже готовые вирусы любых возможностей и средства для автоматического создания вирусов необходимой функциональности и разрушительной силы. Хотя сами вредоносные программы и средства для их создания менее распространены, чем советы и рекомендации для создания вредоносных программ, чуть ли не каждая десятая страница, найденная по запросу «как создать вирус» в различных поисковых системах, позволяет скачать программу вредоносного характера.

Большинство советов и средств как для вирусосоздателей, так и для взломщиков компьютерных систем содержалось на специализированных порталах, рассчитанных на компьютерного преступника, сайтах «все для хакера». На подобных порталах в ходе проведенного исследования были обнаружены не только информация и средства, способствующие совершению преступлений в сфере компьютерной информации, но и руководства по другим видам преступлений, которые можно осуществить посредством Интернет, таким как «Незаконное распространение порнографических материалов или предметов» (ст. 242 УК РФ); «Мошенничество» (ст. 159 УК РФ); «Нарушение авторских и смежных прав» (ст. 146 УК РФ) и т.д.

Таблица 14

Данные, полученные в результате запроса «Все для хакера» (по состоянию на октябрь 2006 г.)

Представляется, что распространенность и доступность подобных сайтов в Интернет отражает популярность среди русскоязычных пользователей Глобальной сети информации, помогающей совершать компьютерные и Интернет-преступления. Кроме этого, огромное количество публикуемых статей по взлому свидетель-

ствует о том, что в российском Интернет хватает специалистов, знающих, как осуществить взлом не на уровне новичка, и не только обучившихся взлому, но и способных этому обучить других.

Представляется, что для выяснения тенденций изменения количества таких деяний необходимо взять Интернет-срез преступности через определенные интервалы времени, чтобы получить данные об уменьшении или увеличении числа сайтов, публикующих информацию, рассчитанную на Интернет-преступника, и на основе этих данных сделать прогноз дальнейших изменений показателей.

Таблица 15

Результат повторных запросов
(по состоянию на февраль 2007 г.)

Поисковая система	Yandex.ru	Rambler.ru	Google.ru
Запрос	Количество найденных страниц/ Количество найденных сайтов	Количество найденных страниц/ Количество найденных сайтов	Количество найденных страниц/ Количество найденных сайтов
как взломать сайт	162 721/ не менее 1 407	458 985/ 27267	1 590 000 / -
как взломать программу	118 077/ не менее 845	220 592/ 21 212	1 270 000 / -
как взломать компьютер	55 334/ не менее 1 565	17 535/ 153 607	1 210 000 / -
как создать вирус	185 152 / не менее 1 718	441 928/ 27 368	1 730 000 / -
все для хакера	6 552 / не менее 917	4 805 833 / 140529	1 530 000 / -

В результате повторного запроса через 4 месяца мы получили противоречивые данные: во-первых, несколько показателей уменьшилось (по запросу «как взломать сайт» на 38,8% — количество страниц и 19,4% — количество сайтов на Yandex.ru, на 8,4% — количество страниц на Rambler.ru; по запросу «как взломать компьютер» на 4,2% — количество страниц на Rambler.ru; по запросу «как создать вирус» на 8,2% — количество страниц на Rambler.ru, на 34,4% — количество страниц Google.ru; по запросу «все для хакера» на 17,3% — количество страниц на Google.ru), во-вторых, на Google по остальным запросам количество страниц увеличилось

многократно, запрос «как взломать сайт» — в 2,75 раза, «как взломать программу» — в 2,8 раза, «как взломать компьютер» — в 4 раза. Заметим также, что когда одни показатели в одних поисковых системах увеличиваются, в других они уменьшаются или остаются практически такими же. На основании повторного исследования мы пришли к выводу, что такое непоследовательное и крайне существенное изменение числовых характеристик свидетельствует о том, что методы поиска и алгоритмы выборки в «поисковиках» меняются крайне динамично. Данный факт в настоящее время не позволяет говорить о поисковых системах как средстве изучения динамики изменения количества общественно опасной информации в сети, так как поисковые системы активно меняют механизмы поиска в конкурентной борьбе за пользователей с целью повышения эффективности поиска; но все же отметим, что поисковые системы позволяют отразить структуру и текущее состояние Интернет.

Если еще 5 лет назад отмечался только огромный криминогенный потенциал сети[113], то в настоящее время этот потенциал раскрылся. Список преступлений, которые можно совершать посредством Интернет, достаточно широк, хотя есть возможности для дальнейшего его роста. Кроме этого, необходимо отметить высокую латентность Интернет-преступности, что не позволяет реально оценить ее размах. Хотя косвенные данные и исследования, проведенные нами, свидетельствуют о широкой распространенности преступлений в русскоязычном Интернет.

2.2. Криминологический анализ отдельных видов Интернет-преступности

Несмотря на то, что огромное значение имеет количественный показатель состояния преступности, который можно сравнить с другими видами общественно опасных деяний, важна и качественная ее характеристика — структура преступности. Нередко структуру называют мерой общественной опасности преступ-

[113] Кесареева Т.П. Криминологическая характеристика и предупреждение преступности в российском сегменте сети Интернет: дис. ... канд. юрид. наук: 12.00.08. — М., 2002. — С. 34.

ности[114]. Она характеризуется удельным весом тех или иных подвидов преступлений, соотношением преступлений небольшой тяжести, средней тяжести, тяжких и особо тяжких, удельным весом преступлений экономической направленности, ценой преступности (т.е. величиной ущерба) и т.д. Уровень распространенности наиболее общественно опасных категорий преступлений, которые преобладают в структуре преступности отдельного государства, является важнейшим показателем оценки его криминализированности.

Представляется, что структура Интернет-преступности сильно отличается от соотношения подвидов преступлений в Глобальной сети, полученного из официальной статистики. В структуре Интернет-преступности наибольший вес в Российской Федерации имеют преступления в сфере компьютерной информации (Глава 28 УК РФ); про другие преступления, совершаемые посредством Интернет, информацию из официальных источников получить очень сложно. Кроме преступлений в сфере компьютерной информации и мошенничества, в Интернет распространены другие виды преступлений, совершение которых возможно и без помощи Интернет, но Глобальная сеть в силу своей природы облегчает злоумышленнику задачу.

Эти сегменты преступности в Глобальной сети можно выделить в структуре Интернет-преступности в отдельные подвиды. Согласно официальной статистике зарегистрированных преступлений, вес таких видов в преступности в Глобальной сети и в преступности в целом либо очень невелик, либо данные об этом отсутствуют. Но проведенные нами исследования показывают, что распространенность Интернет-ресурсов, связанных с этими видами преступной деятельности, достаточно высока.

Благодаря таким свойствам Глобальной сети, как наднациональный характер, отсутствие явно выделенного центра, анонимность, доступность в любой точке мира и возможность совершения операций за доли секунды, Интернет притягателен для использования организованными преступными группами и отдельными преступ-

---

[114] См: Криминология: учеб. пособие / Г.И. Богуш и др.; под. ред Н.Ф. Кузнецовой. — М.: ТК Велби, Изд-во Проспект, 2006. — С. 51; Криминология: Учебник / под. ред. В.Н. Бурлакова, Н.М. Кропачева. — СПб.: Санкт-Петербургский гос. ун-т., 2002. — С. 47 — 51 и др.

никами. Возникли не только новые виды преступлений, направленных на компьютерные системы, но и существующие их виды получили возможность для совершения более безопасно, быстрее и дешевле. Для преступности, как и для легальной деятельности, стерлись национальные границы. В Интернет в связи с его быстрым развитием появились негативные явления, которые вряд ли можно определить как преступность, так как они состоят из деяний, не запрещенных УК РФ, но представляющих серьезную общественную опасность. Данные явления непосредственно связаны с Интернет-преступностью и носят распространенный характер.

Для понимания процессов, протекающих в таком сложном негативном социальном явлении, как Интернет-преступность, необходимо рассмотреть отдельные ее подвиды. Наиболее часто совершаемыми являются: распространение порнографии и еще не криминализованный спам. Кроме выделенных, также существуют виды, которые не имеют такого широкого распространения в Интернет, но сопутствуют крайне опасным видам преступности не в виртуальном, но реальном мире, таким как наркопреступность и терроризм. В ходе нашего исследования была предпринята попытка проанализировать характеристику как наиболее распространенных подвидов Интернет-преступности (спам, распространение порнографии), так и подвидов менее распространенных, но являющихся частью явлений, которые представляют большую опасность (наркопреступность и терроризм).

Наркопреступность в Интернет. Если еще в начале 20 века проблема наркомании была знакома в мире только узкому кругу специалистов, то в конце 20 века, а тем более в 21 веке, она превратилась в глобальную, транснациональную проблему, представляющую угрозу всему мировому сообществу. Но даже когда наркомания и наркопреступность в середине 20 века стали принимать угрожающие размеры в тех или иных государствах, — это были национальные проблемы. В настоящее время наркопреступность и наркомания приобрели международный характер. Это во многом связано с глобализацией финансовых, банковских, торговых, технологических, информационных процессов. Революция в области компьютерных технологий привела к тому, что в современный период проблема распространения наркотиков и наркомании в мире все чаще пересекается с возможностями современных тех-

нологий, в том числе Интернет[115], значение которого в настоящее время огромно.

Посредством Интернет в любую точку мира можно послать информацию о купле-продаже наркотиков, о новых разработках в изготовлении, культивации, их транспортировке и т.д. Интернет дает возможность установить контакты между производителями наркотиков и их распространителями из географических пунктов довольно-таки удаленных друг от друга. Глобальная информационная сеть позволяет также лицам, заинтересованным в распространении наркомании, вовлекать пользователей Интернет в употребление наркотиков напрямую, и популяризировать субкультуры, прямо или косвенно связанные с потреблением наркотиков.

Заметим, что официальная статистика по наркопреступности в сети Интернет просто отсутствует, хотя опасность данного вида преступности не поддается сомнению. Провести полный анализ сайтов в Интернет, связанных с наркотиками, затруднительно как экономически, так и технически в силу огромного объема информации, содержащейся в Интернет; к тому же такое исследование требует не количественного, а качественного анализа сайтов, что также представляет сложности для технической реализации.

В настоящее время наиболее удобным и используемым способом поиска информации являются поисковые серверы. Анализ ссылок, предоставляемых поисковыми серверами, позволяет получить представление о доступности той или иной информации, о количестве обращений к Интернет-ресурсам и о вероятности того, что человек, ищущий информацию о наркотиках любого рода, попадет на тот или иной сайт.

В ходе проведенного нами исследования в качестве поисковых серверов были выбраны крупнейшие российские сервера Yandex.ru, поисковую службу которого за апрель 2005 г. посетили с 2 496 040 Интернет-адресов 15 607 486 раз, обратившись с поисковыми запросами 552 343 666 раз[116], и Rambler.ru, поисковую службу и основную Интернет-страницу которого за май 2005 г. посети-

---

[115] См. например: Schweitzer D. Incident response: computer forensics toolkit. — Wiley, 2003. — P. 44.

[116] Посещение служб Яндекса [Электронный ресурс]/ yandex.ru. — Режим доступа: http://stat.yandex.ru/?Age=m&sort=5&SDay=0&FDay=0&SMonth=0&FMonth=0&SYear=2000&FYear=200

ли с 14 855 120 Интернет-адресов 33 004 288 раз, обратившись с поисковыми запросами 199 862 188 раз[117]. Процедура исследования описана выше в разделе криминологическая характеристика Интернет-преступности.

Согласно полученным данным (17 мая 2005 г.), с использованием контент-анализа первых 100 ссылок на запросы «продаю наркотики», «изготовить наркотики» были установлены следующие факты. Ссылки на Yandex.ru при обработке запроса «продаю наркотики» в 90% случаев оказались страницами Интернет СМИ, правда при этом в 12% от общего числа ссылок согласно рекомендациям, выработанным ООН для журналистов, освещающих проблему наркомании, можно признать приносящими вред[118], т.е. ссылками на публикации, которые прямо или косвенно вызывают интерес к употреблению наркотиков и побуждают человека участвовать в противоправной деятельности, связанной с оборотом наркотиков.

Например, информация о высоких доходах наркопреступников может вызвать побуждение к занятию данным противозаконным видом «бизнеса». 3% оказались сайтами и форумами для наркоманов, на которых пользователи Интернет могли получить информацию, как изготовить и где купить наркотики (дальше по тексту «сайты для наркоманов»). Остальные сайты либо не связаны с наркотиками, либо это медицинские порталы, где наркотические средства упоминаются в контексте медицинских средств и возможностей лечения.

На поисковом сервере Rambler.ru при аналогичном запросе в числе первых 100 ссылок оказалось 2% «сайта для наркоманов»,

---

[117] Статистика сервера [Электронный ресурс] / Rambler.ru. — Режим доступа: http://top100.rambler.ru/top100/Rambler/rate5.0.shtml.ru

[118] «Ваша публикация принесет вред или приведет к отрицательным последствиям в следующих случаях: использование неточной или вводящей в заблуждение терминологии в отношении наркотических средств, как, например, искусственное разделение на так называемые «сильные» и «слабые» наркотики, так как все они запрещены конвенцией ООН; сообщения о потреблении наркотиков людьми, добившимися успеха или славы в обществе; восхваление наркотиков в песнях, кинофильмах, других коммерческих произведениях; привлечение внимания людей к огромным прибылям, которые могут быть получены от незаконной торговли наркотиками; выступление за легализацию немедицинского потребления наркотиков» - принятые ООН рекомендации журналисту, пишущему о наркотиках. Доступно из: http://www.narkotiki.ru/mir_5623.html

11% ссылок публикации в СМИ, приносящие вред согласно рекомендациям ООН, всего публикаций в электронных СМИ оказалось 81%.

Представляется, что с помощью Интернет потребители наркотиков могут легко выйти на наркоторговцев, а продавцы наркотиков могут расширить аудиторию, в которой они их распространяют. Еще чаще вероятность найти в Интернет материалы, рекламирующие или пропагандирующие употребление и распространение наркотиков, что влияет на распространение наркомании и наркотизма в обществе.

При обработке запроса «изготовить наркотики» поисковой системой Yandex.ru 10 % оказались публикациями в СМИ, приносящими вред. Всего публикациями в СМИ оказалось 87% ссылок, 5% — ссылки на словарь сленга наркоманов Баяна Ширянова, в котором кроме трактовки сленга, можно найти состав тех или иных наркотиков и способы изготовления. При аналогичном запросе на Rambler.ru ссылок на словарь оказалось такое же количество. Ссылок на другие ресурсы, где предоставлена информация о том, как купить или изготовить наркотики, — 3%, на публикации в СМИ, приносящие вред, приходится 10%. То есть не составляет труда найти материалы, позволяющие изготовить наркотики в домашних условиях из подручных средств. Подробность описания и простота предоставленной информации достаточна для того, чтобы человеку, не искушенному в химии и фармакологии, в домашних условиях получить наркотики.

Также с помощью поисковых систем Rambler.ru и Yandex.ru в мае 2005 г. было найдено 48 русскоязычных сайтов, пропагандирующих употребление наркотиков; предоставляющих информацию о том, как вырастить или изготовить прекурсоры и наркотические вещества. Подавляющее большинство (37 — сайтов, 77%) составляют сайты о конопле и ее производных. При этом на этих сайтах не только пропагандируют, но и активно вовлекают в употребление наркотиков посредством таких интерактивных подразделов, как форумы и чаты.

На многих сайтах есть ссылки на другие пронаркотические ресурсы, то есть попав на один такой сайт, пользователь Интернет попадает в целую сеть наркосайтов. На них не только описывается, как производить наркотики в домашних условиях, но и как уйти от задержания правоохранительными органами и избежать уголов-

ной ответственности, как безопасно создать свою сеть распространения наркотиков и вовлечь других людей в их употребление.

Не представляет технической сложности разместить ресурс на русском языке, вовлекающий в употребление производных конопли, например, в Голландии, где это будет вполне легально. В УК РФ нет статьи, предусматривающей уголовную ответственность за распространение информации о том, как изготовить наркотики в домашних условиях, хотя общественная опасность таких действий высока. Статья за распространение такой информации вне медицинских изданий в Уголовном кодексе РФ была бы эффективной мерой противодействия наркопреступности в Интернет. Заметим, что предпосылки для криминализации подобных деяний уже есть. Во-первых, данная информация, размещенная вне медицинских и других профессиональных изданий, несет очевидную общественную опасность. Во-вторых, согласно проведенным нами исследованиям большая часть опрошенных считает это деяние чрезвычайно опасным и одобряет его криминализацию (70%, 76% и 81 % — в трех группах соответственно, см. § 2.3).

Исследование ссылок, найденных с помощью поисковых машин, свидетельствует о том, что попасть на пронаркотические сайты несложно. На этих сайтах наркоман и наркоторговец могут получить всю необходимую информацию для производства, сбыта, хранения, транспортировки и других операций с наркотиками. Действия по созданию рекламы и распространению подобной информации как в Интернет, так и в СМИ, — не криминализованы, кроме склонения к потреблению наркотических средств (ст. 230 УК РФ).

Представляется, что размещение в Интернет информации, вовлекающей в употребление наркотиков, можно квалифицировать по ст. 230 УК РФ, так как под склонением к потреблению понимают любые умышленные действия, направленные на возбуждение интереса или желания попробовать данные препараты. К ним могут относиться уговоры, просьбы, советы, рассказы о незабываемых впечатлениях от наркотической эйфории, предложение испытать острые ощущения и другие способы, которые зачастую можно встретить на Интернет-сайтах, адресованных наркоманам или желающим попробовать на себе действие наркотиков. Но, как справедливо отмечают некоторые авторы, современные возможности и способы склонения к употреблению наркотических

средств значительно шире и разнообразней тех, что предусмотрены ст. 230 УК РФ. Чего только стоят пронаркотические сайты российского сегмента Интернет[119].

При этом способы пропаганды становятся все более изощренными. Вот например, описание Интернет-игры ganjawars (англ. слег. - марихуановые войны): «Несколько тысяч наркодилеров живут и работают на четырех виртуальных островах. Их основная задача - делать деньги. Любыми способами — работая на предприятиях и плантациях, распространяя траву и другие ресурсы, создавая преступные синдикаты и, конечно, участвуя в уличных боях. Несмотря на общую ганджа-направленность проекта, разработчики усиленно открещиваются от пропаганды наркотических веществ: на сайте то и дело встречаются надписи, которые напоминают игрокам, что наркотики нельзя ни употреблять, ни тем более распространять»[120].

Отметим, что хотя авторы рецензии пытаются защитить доброе имя сайта, такой вид пропаганды очень опасен. Ролевая игра (к которым относится ganjawars) подразумевает полную погруженность в игру, игрок проживает там целую жизнь и часть этой жизни наркотики. То есть в отличие от обычных призывов такой вид десоциализации может быть еще более разрушителен, не только аудио и видео образы, но и активные действия самого игрока дают большую степень воздействия.

Общественная опасность Интернет-сайтов высока также из-за того, что пользователи Интернет в основном молодежь, и сайты доступны из любой точки России, где есть сеть Интернет. Кроме этого, посещение данных сайтов анонимно, а следовательно, в меньшей степени подвержено социальному контролю, что создает дополнительный спрос на подобного рода информацию.

Отсутствие уголовной ответственности и санкций за рекламу и пропаганду потребления наркотиков, а также за распространение информации о том, как изготовить наркотические вещества, не оправданно особенно в настоящее время, когда в России наблюдается рост уровня наркотизации населения. Законодатель в этой связи очень непоследователен, ведь за все операции с нарко-

---

[119] Гузеева О. Склонение или пропаганда? // Законость. — 2008. — № 2. — С. 36 — 37.

[120] http://www.igromania.ru/Articles/11084/Igraem_Ganja_Wars.htm

тическими средствами предусмотрена уголовная ответственность, кроме их рекламирования и пропаганды.

На наш взгляд, за рекламирование и пропаганду потребления наркотиков следует установить уголовную ответственность, так как подобные деяния несут большой общественно опасный вред. При этом более опасной может быть реклама потребления в Интернет из-за масштабного охвата осуществляемой преступником пропаганды. Примеры уголовной ответственности за рекламирование социально опасной деятельности и материалов уже есть, — так, например, ст. 242 УК РФ устанавливает уголовную ответственность не только за незаконное распространение и изготовление порнографических материалов и предметов, но и за их рекламирование[121]. Представляется, что рекламирование потребления наркотических средств не менее общественно опасно, чем реклама порнографии. Эта проблема выходит за рамки Интернет, так как вопрос рекламирования наркотических средств в СМИ стоит не менее остро, хотя за это предусмотрена административная ответственность (Ст. 13.15 КоАП РФ).

Уровень распространенности подобной информации дает основания утверждать, что возможности воздействия административно-правовыми мерами ограниченны. Представляется необходимым рассмотреть юридико-криминологические основания криминализации, которые предложены А.И. Коробеевым[122].

Заметим, что при решении вопроса об общественной опасности рекламирования наркотических средств в первую очередь необходимо учесть тот факт, что противодействие наркотизму и наркопреступности является одним из важнейших направлений уголовной политики Российской Федерации. При этом значительным фактором широкой наркотизации нашего общества является активная пропаганда и рекламирование потребления наркотических средств, а также легитимация ценностей наркозависимых в массах. В этой связи трудно поставить под сомнение значительную общественную опасность этих деяний.

---

[121] См. например: Уголовное право. Особенная часть. Учебник / Под ред. проф. Л.Д. Гаухмана и проф. С.В. Максимова. — М.: Изд-во Эксмо, 2005. — 704 с.

[122] Российское уголовное право. Курс лекций. Том.1. Преступление / Под ред. проф. А.И. Коробеева. — Владивосток: Изд-во Дальневост. ун-та, 1999. — С. 88—89.

Также важно, чтобы криминализация деяний по рекламированию потребления наркотических средств не противоречила принципу экономии репрессии, то есть необходимо рассмотреть вопрос, не может ли данная проблема быть решена в рамках иных отраслей права. Представляется, что статьи, ограничивающие и запрещающие рекламирование наркотиков, существуют в нескольких российских нормативных актах: ст. 4 ФЗ «О средствах массовой информации», ст. 46 ФЗ «О наркотических средствах и психотропных веществах», ст. 6.13 КОАП РФ. Данные статьи за многолетнюю практику использования доказали свою несостоятельность, более того, ставится под сомнение вообще разрешение проблемы борьбы с пропагандой наркотиков мерами административного воздействия. Так, на совещании главных детских наркологов, проводимом Управлением здравоохранения Российской Федерации, было заявлено, что существующие меры не эффективны и решать вопрос путем административных запретов не перспективно[123].

Представляется, что уголовный запрет рекламирования потребления наркотиков не несет серьезных негативных последствий. Польза от противодействия уголовными мерами данному виду деяний больше, чем предполагаемый ущерб для общества и государства в случае простого ограничения свободы распространения информации о наркотических веществах. Более того, сложно найти какие-либо весомые положительные эффекты в противовес негативным. Многочисленные книги, телепередачи, молодежные журналы, Интернет-сайты, даже музыкальные произведения, в которых рекламируется потребление наркотиков, — все это причина высокой наркотизации российского общества.

Выходит, что с юридико-криминологической точки зрения есть все условия для криминализации данного общественно опасного деяния, но вопрос введения уголовной ответственности за рекламирование наркотиков этим не должен ограничиваться. Также необходимо подвергнуть анализу социально-экономические и социально-психологические основания криминализации, дать жесткую формулировку термина «рекламирование» и разрешить дру-

---

[123] Актуальные вопросы антинаркотической пропоганды [Электронный ресурс] // Нет наркотикам. — Режим доступа: http://www.narkotiki.ru/mir_5623.html

гие спорные моменты. Представляется, что рассмотрение этих вопросов выходит за рамки нашего исследования, так как требует отдельного научного изыскания.

Из всего выше сказанного видно, что в современных условиях Интернет — серьезное подспорье наркопреступности. Существует необходимость в таких предупреждающих мерах, как разработка ресурсов по профилактике наркомании в противовес пронаркотическим сайтам, а также создание общественных групп, например, журналистов, для введения добровольных ограничивающих правил публикации в Интернет того материала, который относится к наркомании и наркотизму. К тому же в качестве предупреждающих мер можно предложить административные и уголовно-правовые меры воздействия на компьютерные компании, предоставляющие место под сайты, где размещается информация о наркотиках. Необходимо рассмотреть и некоторые другие некриминализованные общественно опасные деяния, связанные с наркопреступностью в рамках института криминализации.

По нашему мнению, есть предпосылки для внесения изменений с учетом современной ситуации в статью 230 УК РФ, добавив квалифицирующий признак «совершение преступления посредством компьютерной сети» (см. § 1.1.). С целью повышения эффективности борьбы с рекламированием наркотических средств, психотропных веществ или их аналогов предлагаем модель следующей статьи УК РФ:

Ст. 228[3]. Рекламирование наркотических средств, психотропных веществ или их аналогов

1. Незаконные рекламирование или пропаганда наркотических средств, психотропных веществ или их аналогов, —

наказывается ...

2. Те же деяния совершенные посредством публикации материалов в глобальной *компьютерной сети* или средствах массовой информации, —

наказывается ...

В целом наркопреступность в Глобальной сети не должна оставаться без общественного внимания, так как влияние Интернет на социум с каждым годом растет.

Террористическая деятельность в Интернет. Законодатель Российской Федерации в Уголовном кодексе прямо дает опреде-

ление понятия террористический акт[124]. В свою очередь, Интернет-терракт — это совершение таких действий или угроза совершения таких действий посредством Интернет. Интернет-терроризм — это один из подвидов компьютерного терроризма, где используемой компьютерной технологией является всемирно распространенная, вовлеченная практически во все мировые процессы, общедоступная технология Интернет.

Наибольшую опасность терроризм в Интернет представляет для стран, где процент населения, пользующегося Глобальной сетью, превышает 50% и где Интернет активно используется не только отдельными гражданами, но и государственными органами, банковской средой, общественными и неформальными объединениями. Несмотря на то, что сочетание Интернет-терроризм пока звучит непривычно, его активное внедрение и развитие в России в настоящее время становится реальной угрозой.

В России из-за малого количества пользователей и из-за нераспространенности использования Интернет в критических системах, — например, в системах жизнеобеспечения, компьютерный терроризм, в том числе Интернет-терроризм, еще совсем недавно считался не очень актуальным. Интернет еще не до конца внедрился в государственно-политические, военные и экономические инфраструктуры России, и совершение терактов посредством Интернет представляется пока что маловероятным. Представляется, что вследствие роста компьютерной преступности и терроризма в Российской Федерации данная угроза, по оценкам специалистов, будет возрастать.

По формулировке, принятой международным сообществом, терроризм — это заранее продуманное и подготовленное противозаконное (противоправное) применение насилия или его угрозы в отношении личности, групп населения или даже органов власти с целью вынудить их к принятию выгодного для себя решения

---

[124] Это совершение взрыва, поджога или иных действий, создающих опасность гибели людей, причинения значительного имущественного ущерба или наступления иных общественно опасных последствий, если эти действия совершены в целях нарушения общественной безопасности, устрашения населения или оказания воздействия на принятие решений органами власти, а также угроза совершения действия в тех же целях (ст. 205 УК РФ).

либо получения материальных выгод от объекта террора[125]. При этом характерной особенностью терроризма является применение силы в политических целях, что отличает его от подлинно уголовных преступлений.

Например, распространение вируса «I love you» хотя и принесло за первые 5 дней своего появления ущерб в размере нескольких миллиардов долларов, вряд ли можно считать актом Интернет-терроризма, так как вредоносная программа не преследовала политических целей. Несмотря на это, современные террористы вполне могут воспользоваться этим грозным оружием, так как данный вирус можно легко достать на хакерских сайтах, для этого достаточно ввести в поисковой системе Yandex.ru фразу «исходник[126] I love you» (фраза на компьютерном сленге означает — «компьютерный код программы вируса I love you»).

По нашему мнению, терроризм в Интернет неоднороден, его можно разделить на две составляющие: во-первых, совершение терактов посредством Интернет и, во-вторых, деятельность, способствующая терроризму, скажем, вербовка в организации, сбор средств для террористов или организация взаимодействия между членами террористических групп.

Так, например, против аэропортов США кибертерроризм может быть использован самыми различными способами. От самого простого варианта — как средства для дезинформации и психологической атаки посредством сообщений о различных угрозах, что вносит хаос в работу аэропорта и самолетов, также и в форме кибертерроризма в виде фатальных происшествий и угрозы повреждений аэропортов и самолетов в воздухе[127]. Совершение терактов посредством Интернет наиболее опасно для стран, в которых Интернет активно внедрен во все сферы деятельности, к этим государствам относятся США, члены ЕС, Япония, Южная Корея и т.д.

Для российского Интернет, находящегося в стадии развития, характерен второй вариант террористической деятельности, то

---

[125] Лунев А.А. Терроризм как объект криминологического изучения: дис. ... канд. юрид. наук: 12.00.08. — Ростов-на-дону, 2004. — С. 16—17.

[126] Исходник — на программистском сленге исходный код программы.

[127] Кибертерроризм — самая серьезная угроза для гражданской авиации / Под ред. Щуко // Борьба с преступностью за рубежом. — 2001. — № 11. — С. 11—12.

есть действия, неотделимые от терроризма и способствующие его росту, а также препятствующие борьбе с этой угрозой. Представляется, что это связано с тем, что Интернет в России пока мало используется в системах, от которых зависит жизнь людей, а чаще — как средство поиска информации. Кроме того, данные деяния не наказуемы уголовно и менее осуждаемы общественно и поэтому не обращают на себя должного внимания.

Представляется, что Интернет в данном случае выполняет два вида функций: распространение информации протеррористического толка и инструментальную.

Информация, размещенная на русскоязычных сайтах, принадлежащих террористическим организациям, либо объединениям, сочувствующим террористам, может преследовать самые разные цели и адресована самой различной аудитории. Согласно нашему исследованию, аудитория была разделена на подвиды по степени отношения к терроризму и анализировалось, на кого чаще рассчитана информация. Исследовались только русскоязычные варианты сайтов и располагающиеся на основной странице тексты. Представляется, что варианты сайтов на арабском языке могут чаще обращаться к потенциальным членам и сочувствующим, чем к широкой общественности. Нередко тексты начинались как обращение к широкой общественности с легитимацией действий террористов, а заканчивались прямыми призывами к вступлению в террористические организации и оказанию финансовой помощи терроризму.

Согласно нашему исследованию[128], протеррористическая информация, распространяемая в Интернете, предназначается для: членов террористических организаций — 5,61%; потенциальных членов — 29,91%; сочувствующих — 40,19%; широкой общественности — 71,02%; противников террористической деятельности — 13,08%.

Информация, предназначенная для членов террористических организаций, может преследовать различные цели: информационную, то есть информирование членов организации о событиях

[128] Мы исследовали 168 протеррористических и пронационалистических сайтов, в том числе: http://kavkaz.tv, http://www.tropagneva.com/, http://true1.boom.ru/, http://www.jamaat.ru/, http://soprotivlenie.marsho.net/, http://bratstvo.info/index.php?newlang=ru, http://rko.cjb.net/ и др.

внутри и за пределами группировки; организационную — для установки взаимодействия между членами организации; идеологическую, методическую и другие[129].

Цель информации, направленной на потенциальных членов и сочувствующих, завербовать новых людей и найти поддержку в другой форме, например, материальной. На сайте, поддерживающем терроризм, «Kavkaz.tv», предлагается сотрудничество журналистам[130], которые пишут происламские материалы, осуждающие политику России по борьбе с терроризмом.

Материалы, рассчитанные на широкую общественность, также выполняют самые разные цели, в результате анализа содержания главных страниц сайтов мы получили следующие цифры:

- легитимация действий и идеологии — 91,7%;
- реклама террористических организации — 48,2%;
- оскорбление — 13,7%;
- устрашение — 11,3%.

Стремясь повлиять на общественное мнение, на протеррористических сайтах не используется слово «террористы», а вместо него такие слова, как «борцы за свободу», «бойцы сопротивления», «партизаны», «творцы свободы», даже «истинные демократы» и т.д. При описании террористических операций применяются термины «сопротивление», «вооруженная борьба» и другие. Террористическим актам придается «законный вид» при помощи демонстрации жестокости противника. Известные террористы выдаются за религиозных «мучеников» и приравниваются к «святым».

Устрашение всегда сопровождается оскорблениями и унижающими достоинство фразами. А иногда в послании преследуются все цели сразу, — так, например, в одном из посланий[131] на сайте «ТРОПА ГНЕВА» сначала рассказывается о якобы нацисткой политике России на Кавказе и зверствах скинхэдов (легитимация), затем заявляется о бескорыстной, аполитичной борьбе за свободу (реклама), и в конце говорится о том, что русские, не

[129] Например, на сайте Рамзана Ахмадова можно было найти интервью с Шамилем Басаевым и видеозаписи терактов.

[130] http://kavkaz.tv/russ/sotrud/

[131] http://www.tropagneva.com/242533.asp?=news=detail

признающие ислам, — это болезнь, обреченная на гибель (устрашение)[132].

Материалы для противников террористических организаций могут также преследовать цели устрашения, оскорбления чести и достоинства личности. Так, на некоторых порталах то и дело появляются угрозы, адресованные сотрудникам российских правоохранительных органов и военнослужащим РФ. Нередко такие угрозы сопровождаются видеоматериалами расстрелов и словесным описанием того, что делают с противниками террористических организаций.

По нашему мнению, деятельность в Интернет, не связанную с размещением информации, также можно подразделить на виды:

- непосредственная вербовка в террористические организации;
- осуществление коммуникаций между членами групп;
- сбор сведений для осуществления террористической деятельности и подготовки терактов;
- распространение средств для совершения актов Интернет-терроризма.

Оценить размах этой деятельности представляется сложным. Сайты вербовки и распространения средств сложно найти в обычной поисковой Интернет-системе, так как зачастую доступ к ним открыт только для членов террористической организации. Коммуникации террористов и сбор сведений также сложно отследить, так как Интернет дает возможность передавать данные в шифрованном виде, чем и пользуются террористы. Кроме того, как справедливо замечает Б.Г. Мирзоев, информация протеррористического толка носит часто завуалированный характер, что осложняет выявление подобных ресурсов[133].

Немалую угрозу представляет и возможность сбора информации террористами посредством Интернет. В январе 2003 г. министр обороны США Д. Рамсфельд в прямом послании к армейским под-

---

[132] Интернет позволяет сопроводить такую информацию видеороликами с демонстрацией деятельности террористической организации и звуковыми файлами с записью выступлений известных террористических лидеров. Такое представление информации увеличивает ее общественную опасность, так как более привлекательно и запоминаемо для людей, просматривающих сайт.

[133] Мирзоев Б.Г. Киберпреступность: угрозы безопасности информационного общества // Современное право. — 2006. — № 1. — С. 16.

разделениям предупредил, что слишком много незасекреченного, но потенциально могущего причинить вред материала размещено на сайте Министерства обороны. Рамсфельд напомнил военным, что найденное в Афганистане пособие Аль-Каиды говорит: «используя открытые ресурсы, можно собрать как минимум восемьдесят процентов информации о враге». По его словам, «более 700 гигабайтов информации на сайте Министерства обороны содержат информацию о планах, программах министерства и его действиях. Мы должны подразумевать, что враги имеют регулярный доступ к сайту». Кроме информации, предоставляемой вооруженными силами в Интернет, в свободном доступе есть данные о местонахождении и работе ядерных реакторов и связанного с ними оборудования, что после 11 сентября вызывает беспокойство у публичных деятелей[134].

Хотя оценить соотношение распространенности террористической деятельности в Интернет и в реальном мире достаточно трудно, очевидно, что Интернет дает существенные преимущества террористическим организациям и другим пособнического характера. С ростом внедрения Интернет в жизнь российского общества и его использования в критических системах растет риск удаленной террористической атаки. Под щитом лозунгов «свободы слова» экстремистские организации зачастую ведут работу по воздействию на русскоговорящих граждан.

Распространение порнографии. Бесконтрольное распространение информации в сети способствовало широкому развитию индустрии порнобизнеса. По оценке журнала Forbes, в этой сфере ежегодный оборот составляет 2 — 2,5 млрд долларов, разумеется, что эта цифра касается абсолютно законного (в США, Голландии и многих других странах продажа и изготовление порнопродукции легальны) распространения[135]. Кроме легального и в установленном порядке распространения в некоторых зарубежных странах

---

[134] Maura Conway. Terrorist "use" of the Internet and Fighting back. Paper prepared for presentation at the conference. [Электронный ресурс]/ Oxford Internet Institute University of oxford. — Режим доступа: http://www.oii.ox.ac.uk/research/cybersafety/extensions/pdfs/papers/maura_conway.pdf

[135] Александр Кондратьев. Порно, спам и пиратская музыка: кто и как зарабатывает на них в Интернете // Forbes. — 2006. — № 3 (март). — С. 47 — 54.

порнографии для лиц, достигших совершеннолетия, Глобальная сеть стала рассадником теневого порнобизнеса.

Согласно оценкам некоторых экспертов 40% пользователей Интернет посещают порносайты; около четверти из них являются потребителями детской порнографии. Доля российской детской порнографии на платных сайтах мирового Интернета сегодня составляет более половины от общего объема такой продукции. По оценкам зарубежных экспертов, раскрученный порнографический сайт приносит доход до 2 млн долларов ежегодно. Владельцы самых известных ресурсов заявляют, что их прибыль составляет от 500 до 1000%[136].

В РФ любое незаконное распространение порнографии является уголовно наказуемым деянием, но все же наибольший вред порнография приносит неокрепшей психике подростков и детей. В связи с этим Т.П. Кесареева выделяет несколько связанных с этим проблем: бесконтрольный доступ несовершеннолетних к порнографическим сайтам в Интернет; распространение детской порнографии; сбор информации о детях, которая может быть использована против них[137].

Представляется, что огромные доходы от теневого порнобизнеса стимулируют развитие другой криминальной деятельности в Интернет. Например, незаконный порнобизнес дает работу большому числу хакеров и вирусописателей, так как для ухода от правоохранительных органов организаторы нелегальных сайтов часто пользуются их услугами. Распространение порнографии во многих случаях достаточно сложное преступление и поэтому осуществляется целыми группами соучастников, среди которых есть представители Интернет-преступников разных специализаций.

Порнографические материалы распространяются не только через Интернет, но, по мнению С.В. Молчанова, вред от *Интернет-порнографии* во много раз опасней. Не вызывает сомнений, что размещение на сайтах порнографических материалов нару-

---

[136] Репецкая А.Л. Российский криминальный рынок услуг: структура и характеристика отдельных видов // Криминологический журнал Байкальского университета экономики и права. - 2008. — № 1. — С. 33.

[137] Кесареева Т.П. Криминологическая характеристика и предупреждение преступности в Российском сегменте сети Интернет: дис. ... канд. юрид. наук: 12.00.08. — М., 2002. — С. 88.

шает сложившиеся в обществе стандарты морали. Надо признать, что серверы с такой информацией посещаются в том числе детьми и подростками. Ведь посредством Интернет гарантируется куда большая анонимность и конфиденциальность, чем посещение кинотеатров и магазинов с открытой или подпольной литературой, или порновидеофильмами. Практически отсутствует риск быть узнанными или замеченными[138]. Это вызвано свойствами самой сети и характерно практически для всех видов Интернет-преступности. Отсутствие социального контроля приводит к тому, что потребители незаконной, аморальной, безнравственной информации не боятся оусждения.

Так, согласно нашим исследованиям, распространение детской порнографии гражданами осуждается и воспринимается крайне негативно (около 90% опрошенных нами респондентов высказались, что считают данную информацию опасной и вредной), но анонимность Интернет позволяет потребителям данной незаконной информации оставаться в тени. Выходит, что Интернет сильно увеличивает спрос на подобную продукцию, так как многие из потребителей порнографии не решились бы просматривать ее открыто.

Порноиндустрия глобальной информационной сети и Интернет-преступность неразделимы, об этом свидетельствует также и то, что за последние 4 года 3 номера популярного среди сетевых преступников журнала «Хакер» посвящены тому, как организовать свой порнобизнес и свою порностудию[139]. В них подробно описано, как наладить производство порнопродукции, как уйти от проблем с законом, и какие прибыли крутятся в этой сфере деятельности.

Выгодность этого незаконного бизнеса привела к бурному росту данного вида правонарушений в Глобальной сети. Так, если в 2000 г. речь шла о 70 сайтах в российском Интернет с педофильс-

---

[138] Молчанов С.В. Административно-правовые основания ограничения конституционного права человека на распространение информации через Интернет в Российской Федерации: дис. ... канд. юрид. наук: 12.00.14. — М., 2005. — С. 40.

[139] См: журнал «Хакер» февраль 2002 г., тема номера «Как продаться в порнобизнес», журнал «Хакер-спец» за июнь 2004 статья «Практический курс начинающего порнобарона», журнал «Хакер» за июнь 2004 статья «Организуем свою порностудию».

кой тематикой (75% детской порнографии распространялось через Интернет к 2002 г.)[140], то в 2006 г. количество русскоязычных порносайтов перевалило далеко за тысячу, и они уже практически не поддаются количественному анализу. Например, при вводе в строку поиска в популярной поисковой системе Yandex.ru запроса «порно» (14 декабря 2006 г.), находится не менее 3 387 сайтов и 7 151 071 Интернет-страниц, а вводят всего данный запрос за месяц 2 637 880 раз. Мы специально употребили термин русскоязычных, так как многие сайты физически распространены за пределами Российской Федерации, где некоторые действия, сопряженные с порнографией, не запрещены законом. То есть в настоящее время Интернет основной способ распространения порнографии.

Детская порнография является одним из наиболее общественно осуждаемых видов распространяемой порнографии. Как отмечают специалисты, хотя систематических исследований отдаленных социально-психологических, медицинских и иных последствий участия детей в порнобизнесе не проводилось, однако, судя по результатам клинических наблюдений, то, что им пришлось испытать, оставило глубокий негативный след в их сознании, а у 75% детей наблюдались ярко выраженные нарушения психологической и социальной адаптации[141]. Кроме того, изобилие материалов околопедофильской тематики может вызвать равнодушие и привычку общественности к этой негативной стороне Интернет[142].

Согласно нашему исследованию общественного мнения у большинства опрошенных наблюдается негативное отношение к распространению порнографии (81,8% — среди компьютерных специалистов, 68,6% — среди не компьютерщиков, использующих

---

[140] Кесареева Т.П. Криминологическая характеристика и предупреждение преступности в российском сегменте сети Интернет: дис. ... канд. юрид. наук: 12.00.08. — М., 2002. — С. 93; Сухаренко А.Н. Распространение детской порнографии через сеть Интернет [Электронный ресурс]/ Владивостокский центр исследования организованной преступности. — Режим доступа: http://www.crime.vl.ru/index.php?p=1077&more=1&c=1&tb=1&pb=1# more1077

[141] Петросян О.Ш. Уголовная ответственность за изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних: дис. ... канд. юрид. наук: 12.00.08. — М., 2005. — С. 51.

[142] Например, не редки случаи размещения в Интернет анекдотов и шуток на эту тему, к которым относятся лояльно, а иногда даже приветственно.

Интернет, и 80,5% — среди людей, не пользующихся Интернет, считают распространение порнографических материалов среди несовершеннолетних вредным, см. § 2.3), и еще более негативную оценку получает детская порнография (96,97, 89,66 и 95,24% считают вредным распространение детской порнографии). Несмотря на некоторые высказывания, что общественная опасность порнографии в связи с переоценкой ценностей, существовавших в советском обществе, утрачивает свою очевидность, несомненно, что распространение порнографии несет существенный вред.

Единого мнения нет и среди специалистов, посвятивших данному вопросу диссертационные исследования. Например, М.В. Денисенко говорит о том, что многие люди, сравнивая свои собственные возможности и сексуальные «образцы» могут испытывать чувство личной ущербности и несоответствия стандарту, но в то же время он приводит доводы в пользу того, что порнография не вызывает развития извращений и не стимулирует совершение преступлений на сексуальной почве. За исключением случаев, где порнографическому материалу сопутствуют сцены насилия[143].

Вынуждены с этим не согласиться, распространение порнографии несет огромный негативный эффект. О.А. Булгакова считает, что в настоящее время распространение порнографических материалов тесно взаимосвязано с сексуальной эксплуатацией женщин и детей, выступает катализатором ряда половых преступлений, способствует общему упадку нравственности. К тому же в последние десятилетия это общественно опасное деяние стало довольно прибыльным видом криминальной деятельности транснациональной преступности[144].

А С.В. Молчанов согласен, что систематическая, информационно насыщенная и объемная публикация вообще всех материалов сексуального содержания, направленная на подростков, угрожает гармоничному формированию личности, ее высших социальных потребностей, что чревато гипертрофированным развитием одних сфер индивиду-

---

[143] Денисенко М.В. Уголовная ответственность за незаконное распространение порнографических материалов или предметов: : дис. ... канд. юрид. наук: 12.00.08. — М., 2004. — С. 20—21.

[144] Булгакова О.А. Уголовная ответственность за незаконное распространение порнографических материалов или предметов: : дис. ... канд. юрид. наук: 12.00.08. — Ставрополь, 2003. — С. 4—5.

ального сознания за счет других. В итоге широкая гамма чувств, эмоций, отношений, связанных с социальным феноменом любви, заужива-ется до уровня физиологии и техники секса[145]. Представляется, что широкий размах порнобизнеса в Интернет еще более усиливает моральное разложение общества, стимулирует рост преступности и дискредитирует такие духовные ценности, как любовь и семья. У молодежи наблюдается большая терпимость к распространению порнографии, что свидетельствует об уже наступивших последствиях засилья этой аморальной, противозаконной информации.

Более того возбуждение раннего интереса у подростка к сексуальным отношениям позволяет использовать сексуальный стимул в пропаганде и рекламе остального негатива (наркотиков, алкоголя, насилия). Например, сцены употребления наркотиков в кинофильмах сопутствуют сексуальным сценам. Представляется, что сексуальное моральное разложение подростка в большинстве случаев предшествует остальному деструктиву.

Размах распространенности порнографии непедофильской тематики огромен. Так, мы проанализировали содержание 20 популярных развлекательных сайтов[146], которые расположены в общем доступе[147] и не направлены на публикацию порноматериала. Оказалось, что все они содержат рекламу сетевых порталов, распространяющих порнографию и рекламирующих сексуальные услуги, изображения и видео, попадающие под общепринятое определение порнографии, иногда под видом юмористических[148]. Порнографическими материалами наполнены и сообщения электронной почты[149], — так, по исследованиям компании Symantec,

---

[145] Молчанов С.В. Административно-правовые основания ограничения конституционного права человека на распространение информации через Интернет в Российской Федерации: дис. ... канд. юрид. наук: 12.00.14. — М., 2005. — С. 46.

[146] См. например: www.fishki.net, www.warnet.ws и т.д.

[147] Большинство российских компаний, предоставляющих услуги размещения сайтов, не разрешают публиковать порнографические материалы, поэтому сайты размещаются только на специализированных площадках, иногда за рубежом.

[148] Кроме этого, мы нашли материалы националистического и пронаркотического характера, которые также позиционированы как развлекательные.

[149] Гиряева В.Н. Интернет и молодежь: правовые аспекты // Право и информатизация общества. — М., 2002. — С. 167.

опросившей 1000 детей от 7 до 16 лет в 2003 г., 47% получало спам порнографического содержания[150]. К этим данным надо относиться с особой осторожностью, так как компания Symantec занимается разработкой систем компьютерной и Интернет-безопасности, в том числе разрабатывает программные средства для защиты от спама. По мнению Ю. Трунцевского, компьютерные «пираты» наряду с контрафактными фильмами занимаются распространением порнографических картин[151].

Немаловажной причиной такой распространенности является именно использование Интернет. Во-первых, преступник и физически и юридически может вести деятельность на территории других стран, где распространение порнографии не запрещено законом, либо возможности выявить преступника очень скромные; во-вторых, анонимность Интернет создает трудности в установлении личности и местонахождения преступника. В-третьих, представляет сложность отсутствие значительной практики использования электронных доказательств, а также существует возможность практически мгновенного уничтожения либо подлога компьютерных улик.

В настоящее время распространение аморальных и противозаконных материалов в сети достигло невероятных размеров. Уже на новостных сайтах можно встретить ссылки на порнографические или националистические материалы. Излишняя демократия в вопросе распространения материалов сексуального характера, в том числе порнографии, особенно с участием детей, приводит к негативным социальным и нравственно-психологическим послед-

---

[150] Спам — это массовая рассылка сообщений с помощью электронной почты или других средств немедленной рассылки любых сообщений, без явного согласия получателя или даже вопреки его воле. Также спамом называют отсылку сообщений, содержащих вложенные файлы большого размера, без согласия принимающей стороны, в том числе сообщений, содержащих рекламную или агитационную информацию, угрозы и нецензурную информацию, порнографическую продукцию, предложение интим-услуг и т.д.

См., например, Symantec Survey Reveals More Than 80 Percent of Children Using Email Receive Inappropriate Spam Daily. [Электронный ресурс] / Symantec. — Режим доступа: http://www.symantec.com/press/2003/n030609a.html.

[151] Трунцевский Ю. Общая характеристика составов преступлений, сопряженных со ст. 146 УК РФ в аудиовизуальной сфере // Уголовное право. — 2003. — № 1. — С. 49.

ствиям. Так, например, по мнению социологов, широкая распространенность порнопродукции непосредственно влияет на практическое вымирание института брака, что, в свою очередь, влияет на демографическую проблему, решение которой является одним из приоритетов российского государства.

Слепое копирование западных ценностей приводит к уничтожению российской культуры, ведет к всеобщей аморализации общества, что является причиной роста преступлений. Распространение порнографии в Интернет носит чаще всего навязчивый характер, — так, например, на сайтах непорнографической тематики зачастую в небольшом участке экрана (такие участки называются баннерами (англ. — banner, по аналогии с наружной рекламой) показываются обнаженные части тела или воспроизводится текст порнографического характера, то есть без своего желания посетителям приходится смотреть материалы, запрещенные к открытому распространению в Российской Федерации. При этом практически во всех учебниках по российскому уголовному праву подчеркивается, что даже рекламирование, а не только распространение порнографических материалов, непосредственно уголовно наказуемо[152].

Спам. В последние годы появляется большое количество новых видов опасных деяний, совершаемых в Интернет, которые в настоящее время не криминализованы, так как их общественная опасность не так очевидна, растянута во времени или наносит относительно небольшой материальный ущерб конкретному человеку. В то же время, если брать моральный ущерб или вред, наносимый этими деяниями организациям или целым государствам, то размах негативных последствий очень велик и не всегда в полной мере поддается оценке. Самым распространенным и противоречивым из таких явлений является *спам, то есть массовая рассылка сообщений с помощью электронной почты или других средств посылки любых электронных сообщений* (IRC — Internet Relay Chat, SMS — short message service[153], ICQ — I seek you и т.д.) без явного

---

[152] Уголовное право. Особенная часть: Учебник / Под ред. проф. Л.Д. Гаухмана и проф. С.В. Максимова. — М.: Изд-во ЭКСМО, 2004. — С. 428.

[153] Лазарева И.В. Расследование преступлений, связанных с несанкционированным доступом к сети сотовой радиотелефонной связи: автореферат на соискание степени ... канд. юрид. наук: 12.00.09. — Иркутск, 2007. — С. 16.

согласия получателя или даже вопреки его воле (как, например, в подписке на рассылку новостей).

К спаму относят размещение в Интернет-конференциях (форумах, списках рассылки, сайтах объявлений) любых сообщений, не относящихся к тематике конференций, в том числе размещение рекламных и агитационных сообщений, если это не указано в ее правилах. Спамом является также добавление файлов с приложениями на форум, кроме случаев, когда это указано в самих правилах публикации. Также спам — это рассылка любой электронной информации, когда получатель явно выразил свое нежелание получать данную информацию.

Данный вид деяний в России нельзя отнести к Интернет-преступности с уголовно-правовой точки зрения, так как навязчивая рассылка по электронной почте в настоящее время не запрещена уголовным законом и спам не является преступлением. Несмотря на это, спам как вид деятельности является на данное время неотъемлемой частью Интернет-преступности — так считают и сами компьютерные преступники. На так называемых порталах «для хакеров» наряду со способами взлома и создания вирусов публикуются способы рассылки спама по электронной почте. Более того, Интернет-преступность как социальное явление выходит за рамки только системы уголовно-наказуемой деятельности[154] и включает в себя «поддерживающую» и организационную деятельность. Спам сопряжен с целым рядом уголовно-наказуемых деяний, а также создает рабочие места для Интернет-преступников.

Многочисленные рекламные сообщения, поступающие по электронной почте, в несколько раз превышают количество сообщений действительно необходимых адресату-получателю. По данным, предоставленным коммерческими организациями за 2004 г., в российском сегменте Интернет спам составлял примерно от 75 до 80% всех почтовых сообщений. На серверах крупных публичных почтовых систем количество спам-сообщений еще выше и составляет 85—90%[155]. Необходимо с некоторым недоверием относиться к информации, предоставленной компаниями, так как

---

[154] Номоконов В.А. Актуальные проблемы борьбы с киберпреступностью // Інформаційні технології та безпека. — Киев, 2003. — С. 104.

[155] «Единая Россия» предлагает наказывать спамеров исправительными работами, Lenta.ru, http://lenta2.cust.ramtel.ru/internet/2004/06/25/spam/_Printed.htm (и другие источники)

корпорации, занимающиеся компьютерной безопасностью, зачастую заинтересованы в привлечении внимания к борьбе со спамом, поэтому прибегают к некоторому завышению цифр для увеличения количества продаж средств защиты от спама. Но так как эти цифры не сильно отличаются от мировых (порядка 60 — 70%[156]), то они, скорее всего, актуальны.

Основная часть ущерба от спама приходится на компании, предоставляющие доступ в Интернет и услуги бесплатной почты. Если перевести потери на отдельного пользователя, то ущерб от спама относительно небольшой — от 150 долларов в год и выше. В зарубежных странах этот показатель выше, так как он пропорционален размеру зарплаты и потерянного рабочего времени. Если же рассматривать проблему в масштабах РФ, то это более 250 млн долларов в год, а в мире ущерб превысил 50 млрд. долларов в 2005 г.[157]

Кроме финансовых потерь от спама и потери времени пострадавшего от принудительной рассылки, спам зачастую наносит трудноисчислимый в денежном эквиваленте моральный ущерб. Например, по статистике, приведенной коммерческими организациями, 10 — 30% (колеблется в зависимости от сезона, 18,2% — за 2004 г.) спама являются предложениями по продаже так называемых средств для взрослых (средства повышения потенции и другие продукты интимного характера), которые нередко сопровождаются иллюстрациями с обнаженными женщинами и порнографическим фотоматериалом с соответствующим текстом[158]. Незапланированное увеличение потока писем за счет спама также может вывести или заблокировать как личные почтовые системы, так и почтовые сервера. Такой метод, например, умышленно используют лица с антиобщественной направленностью для остановки работы фирмы-конкурента или создания нарушений в работе государственной службы.

---

[156] Has spam grows stabilized, John E. Dunn, Techworld.com,Wednesday, January 12, 2005 (и другие источники).

[157] См. на сайтах: http://www.spamtest.ru/document.html ?context = 15923&pubid = 19222, http://www.interfax.by/?id = 5_9&arch = 1&arch_id = 23796, http://www.sostav.ru/news/2006/12/13/73/ и т. д.

[158] Спам 2004: аналитический отчет [Электронный ресурс] / Спамтест. — Режим доступа: http://www.spamtest.ru/document.html?context = 15948& pubid = 19223

Многие угрозы, исходящие от спама, еще детально не изучены[159]. Например, спам как средство ведения информационных войн отвечает всем требованиям информационного оружия: скрытность, масштабность и универсальность[160].

Во многих государствах приняты законы против спама (страны ЕС, США и Австралия[161]) и есть практика их применения. Между установленными законодателями уголовно-правовыми мерами, как и между предлагаемыми проектами еще не принятых законов, имеются серьезные различия. Причем эти различия не только в видах и размерах наказания, но и в трактовке понятия спам, а также в подходах к конструированию законов.

Во-первых, представляется, что законы могут быть разделены по объектам регулирования: 1) законы, охватывающие любое нежелательное электронное сообщение, которые запрещают спам в его широкой трактовке, то есть спам в форумах, ICQ и других системах рассылки электронных сообщений (Австралийский Spam Act 2003, директива 2002/58/ЕС Европейского парламента, Data Protection Act 1998 — Великобритания); 2) законы, которые касаются только сообщений электронной Интернет-почты (Американский федеральный закон CAN SPAM 2003 — Controlling the Assault of Non-solicited Pornography and Marketing Act 15 USC 7701 note). Например, в Австралии SPAM ACT 2003 ограничивает *любые* незатребованные (незапрашиваемые) электронные сообщения коммерческого характера (англ. — unsolicited commercial electronic message). Кроме того, *любое* коммерческое электронное сообщение должно содержать информацию о частном лице или организации, пославшей сообщение.

---

[159] Спам зачастую связан с другими общественно опасными деяниями, например, такими, как взлом компьютерных систем для рассылки электронной почты от имени взломанного компьютера или кража баз данных адресов пользователей с последующей перепродажей, заражение вредоносной программой и т.д. Также отметим деятельность, которая сопутствует практически любой рассылке — это предоставление услуг в Интернет, с помощью которых можно сделать рассылку анонимной.

[160] Разуваев В.Э. Правовые вопросы борьбы со спамом как средством ведения информационной войны // Государство и право. — 2006. — № 7. — С. 84—85.

[161] Spam Act 2003 [Электронный ресурс]/ The Attorney General's department. — Режим доступа: http://scaleplus.law.gov.au/html/pasteact/3/3628/top.htm

Напротив, американский CAN SPAM Act 2003 регулирует коммерческие взаимоотношения, накладывая ограничения и вводя санкции за передачу *только* нежелательной *электронной* почты *посредством Интернет* (англ.-Unsolicited commercial electronic mail via the Internet). В свою очередь, Украина ввела уголовную ответственность за спам 23 декабря 2003 г., криминализовав *только* распространение сообщений электросвязи, повлекшее нарушение или прекращение работы электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи (ч. 1 ст. 363[1] УК Украины), что сузило сферу действия закона и позволяет его применять в крайне редких случаях. Поэтому С.О. Заянчуковский называл данную статью «мертвой» нормой[162].

Во-вторых, законы об ответственности за спам различаются по субъектам — так, одни законы касаются только физических лиц, а другие — физических и юридических. Например, в Австралии закон (Spam Act 2003) не распространяется на благотворительные и зарегистрированные политические организации, государственные учреждения, судебные органы, зарегистрированные религиозные организации. В случае рассылки спама подобными организациями данное деяние не считается преступлением.

В-третьих, немаловажный аспект различия — на кого ложится ответственность за рассылку. Спам — это нежелаемая рассылка, в связи с этим существует два варианта трактовки нежелательности. В первом — вся рассылка, на получение которой потерпевший явно не выразил свое согласие, считается спамом («незапрашиваемая рассылка»), при этом электронное письмо с вопросом, «хочет ли потенциальный абонент сети рассылки получать ту или иную информацию», также расценивается как спам. Легитимными признаются такие электронные сообщения, которые пользователь сам тем или иным способом выразил желание получать.

Другой подход тоже основан на трактовке спама как «нежелательной рассылки» или рассылка вопреки воле получателя, но спа-

---

[162] Заянчуковский С.О. Противодействие распространению спама: украинский опыт криминализации // Уголовное право: стратегия развития в XXI веке: материалы 4-й Международной научно практической конференции. — М.: ТК Велби, Изд-во Проспект, 2007. — С. 622—623.

мом считается то, что посылается абоненту вопреки его протесту, выраженному в той или иной форме[163].

Представляется, что посылка вопреки воле получателя, выраженной в конкретных действиях, должна быть юридически запрещена, так как налицо субъективное безразличие спамера к правам другого человека. Даже если рассылка совершается не вопреки воле пользователя, то есть без явного выражения недовольства (например, в первый раз), массовая рассылка, которая замедляет Интернет-трафик, отнимает рабочее время или приводит к другим негативным последствиям, тоже противозаконна. Спамер должен нести ответственность за объемы рассылаемой информации и за вред, причиненный его спамом. Выходит, что нежелательной является как рассылка вопреки явно выраженной воле, так и любая рассылка, приводящая или способная привести к значительным последствиям.

Мнения по поводу введения уголовной ответственности за спам среди ученых и практиков неоднозначны. Противники идеи введения уголовного запрета связывают это прежде всего с ограниченными возможностями средств и методов сбора доказательств, проведения следствия, так как при совершении таких действий может быть нарушено право спамеров на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, а это противоречит общей либерализации и гуманизации общественного законодательства[164].

Ограничение данного права допускается только на основании судебного решения (п. 2 ст. 23 Конституции РФ, ст. 138 УК РФ). Кроме случаев, когда сторона, предоставляющая услуги Интернет

---

[163] Например, Data Protection Act 1998 Объединенного Королевства Великобритания дает право человеку, который недоволен сообщениями прямого маркетинга от какого-либо рассыльщика (англ. — «sender»), выразить в письменной форме нежелание получать сообщения от данного рассыльщика и рассыльщик в разумные сроки должен удовлетворить эту просьбу. К тому же в сообщении должны быть указаны реквизиты, по которым получатель может заявить о своем нежелании получать данную информацию, иначе такое сообщение также считается спамом.

[164] Богдановская И.Ю., Волчинская Е.К. Законодательство о спаме: зарубежный опыт и российские перспективы [Электронный ресурс] // Информационное право. — Режим доступа: http://www.infolaw.ru/lib/2005-1-spam # 15

и электронной почты спамеру, сама инициирует дело против правонарушителя и предоставляет все доказательства, в целом, как нам представляется, уголовный закон не достаточно эффективен. При этом сбор этих сведений без согласия спамера противоречит п. 1 ст. 24 Конституции РФ (сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются). В свою очередь, право спамера на рассылку прямо прописано в Конституции РФ, п. 4. ст. 29: «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом». Данная ситуация выгодна только спамерам, провайдеры же и пользователи Интернет, пострадавшие от спама, практически не защищены законодательно. Представляется, что провайдер, предоставивший информацию о спамерах, сам может быть привлечен к уголовной ответственности по ст. 138 УК РФ, если в договоре об оказании услуг прямо не указано о согласии спамера на ознакомление с его информацией других лиц.

Уголовный закон уже охватывает некоторые наиболее опасные формы спама. Уголовная ответственность возможна при сопутствующем совершении других преступлений, например, к ним относятся:

- распространение порнографических материалов, а также рекламы порнографических ресурсов любым способом, в том числе и по электронной почте (ст. 242 УК РФ);

- неправомерное получение баз данных с адресами электронной почты для рассылки (ст. 272 УК РФ);

- рассылка любых вирусов по электронной почте[165] (именно так распространяются самые опасные вирусы) и распространение их через Интернет-конференции (ст. 273 УК РФ).

Если рассматривать почтовую программу на локальном компьютере частью системы ЭВМ, а почтовые сервера общедоступными системами ЭВМ, то спамера, рассылка которого привела к сбоям в работе почтовых серверов или частной системы ЭВМ, можно считать субъектом преступления по ч. 1 ст. 167 УК РФ, так как способ, которым осуществляется уничтожение или повреждение имущества может быть любым (кроме указанных в ч. 2

---

[165] Хатч Б. Секреты хакеров. Безопасность Linux / Б. Хатч, Д. Ли, Д. Курц; пер с англ. — М.: Издательский дом «Вильямс», 2004. — С. 204.

ст. 167), в том числе и при помощи спама. Признак «значительный ущерб» является обязательным для объективной стороны рассматриваемого состава преступления и относится к категории оценочных. Хотя материальная стоимость сбоя в работе частной системы ЭВМ может быть и невысокой при решении вопроса о наличии в действиях виновного признака значительного ущерба, следует руководствоваться не только стоимостью имущества, но и материальным положением физического лица, а также значимостью утраченного имущества для собственника или иного владельца[166].

По нашему мнению, должны оцениваться также и важность данных, которые уничтожены в ходе сбоя компьютера. В случае с частной ЭВМ это может быть вся личная и деловая переписка, информация, обладающая деловой и материальной ценностью, не подлежащей восстановлению.

Выше приведенные статьи охватывают не все случаи несанкционированной рассылки с наиболее опасными последствиями, хотя УК РФ предусматривает уголовную ответственность за некоторые деяния, связанные со спамом. Представляется необходимым рассмотреть вопрос о криминализации спама, так как многие общественно опасные деяния остаются за рамками УК РФ, а спам в настоящее время является одной из основных и самых распространенных проблем функционирования Интернет.

Для криминализации данного негативного вида деяний необходимы соответствующие «основания». По мнению А.И. Коробеева, данные факторы можно разделить на 3 группы[167].

В *юридико-криминологическую группу* входят следующие основания: 1) степень общественной опасности деяний; 2) относительная распространенность деяний и их типичность; 3) динамика деяний с учетом причин и условий, их порождающих; 4) возможность воздействия на эти деяния уголовно-правовыми средствами

---

[166] Плютина Е.М. Уничтожение или повреждение имущества: проблемы квалификации и соотношения со смежными составами преступлений (по материалам судебной практики Краснодарского края) : дис. ... канд. юрид. наук: 12.00.08. — М., 2005. — С. 77—78.

[167] В книге используется именно термин «основание». Российское уголовное право. Курс лекций. Том.1. Преступление / Под ред. проф. А.И. Коробеева. — Владивосток: Изд-во Дальневост. ун-та, 1999. — С. 88—89.

при отсутствии возможности успешной борьбы менее репрессивными средствами; 5) возможность системы уголовной юстиции.

К *социально-экономическим* основаниям относятся: 1) причиняемый деяниями материальный и моральный ущерб; 2) отсутствие возможных побочных последствий уголовно-правового запрета; 3) наличие материальных ресурсов для реализации уголовно-правового запрета.

Социально-психологическими основаниями являются: 1) определенный уровень общественного правосознания и психология; 2) исторические традиции.

Одним из самых спорных в вопросе криминализации спама является критерий *общественной опасности*. Общественная опасность отражает социальную сущность преступления и выступает основной объективной предпосылкой для установления уголовно-правового запрета на деяние. При этом общественная опасность имеет как количественную, так и качественную стороны. Количественную оценку общественной опасности связывают с понятием степени, а качественную — с характером общественной опасности[168]. Именно преступления в отличие от иных противоправных деяний причиняют значительный или существенный ущерб (реальный или возможный) охраняемым законом объектам.

Несмотря на то, что величина ущерба от спама для одного пострадавшего, от одной незаконной рассылки может быть невелика, однако негативное влияние на общество и экономику государства в целом весьма ощутимо. Кроме этого, отдельная рассылка электронной почты может охватывать большое количество получателей. Выходит, что некоторые рассылки суммарно наносят достаточно большой материальный ущерб. Необходимо учитывать и моральный ущерб, наносимый не только отдельному гражданину, но и в совокупности всем получателям.

По данным нашего исследования, спам не одобряют многие пользователи Интернет. 63,6% респондентов, пользующихся Глобальной сетью и являющихся специалистами в сфере Информационных технологий, считают спам вредной для них информацией; 55,2% из числа опрошенных представителей гуманитарных профессий указали, что спам наносит им вред. Идею установления

---

[168] Уголовное право. Общая часть: Учебник / Под ред. проф. Л.Д. Гаухмана и проф. С.В. Максимова. — М.: Изд-во ЭКСМО, 2004. — С. 91—92.

уголовной ответственности поддержало 40% компьютерных специалистов, и среди «гуманитариев» 24,1% посчитали это приемлемым. То есть большая часть опрошенных выражает явно негативное мнение о спаме, считает его социально вредным явлением, посягающим на их права и интересы. Хотя сама по себе демократическая процедура, то есть принятие во внимание мнения большинства при подготовке законов, не всегда гарантирует их безошибочность, негативное отношение общества является отражением общественной опасности и, следовательно, должно учитываться при криминализации таких деяний.

Необходимо упомянуть и о субъективном источнике общественной опасности спама, который выражается в том, что спам является не просто умышленным, а предумышленным деянием и зачастую выражает злостность спамера, т.к. отсылается вопреки документально выраженному протесту получателя, то есть вопреки его воле. К тому же большое количество спамеров чувствует себя безнаказанно, используя анонимность Интернет.

Например, Калифорнийская компания Blue Secirity предприняла безуспешную попытку борьбы со спамом следующим образом: обнаруживая в почтовом ящике пользователя нежелательное рекламное письмо, программа Blue Frog, разработанная специалистами компании, посылала сотни тысяч жалоб на рекламируемый адрес, чтобы рекламщики задумались, стоит ли в следующий раз пользоваться услугами спамеров. Разослав 552 тыс. писем спамерам с требованием прекратить рассылку рекламы клиентам компании, в результате злоумышленники потеряли возможность хотя бы на время заниматься своей преступной деятельностью, последовал ответ от спамеров, которые находились на территории России. Злоумышленники отправили в компанию Blue Security электронные письма с 10 тыс. компьютеров по всему миру. В результате компании пришлось отказаться от атаки на спамеров. Дополнительным стимулом к этому послужило сообщение, в котором злоумышленники угрожали подвергнуть вирусным и спамерским атакам клиентов Blue Systems[169]. Налицо субъективное пренебрежение спамеров к чужим правам и мерам борьбы, применяемым к ним. Они не

[169] Русские спамеры унизили американскую ИТ-компанию [Электронный ресурс] // Cnews.ru. — Режим доступа: http://www.cnews.ru/news/top/index.shtml?2006/05/17/201473

останавливаются даже при выражении протеста против их деятельности, активно воздействуя на тех, кто им противостоит.

Распространенность данного явления, его типичность вообще не подвергаются сомнению, так как большую часть отсылаемой во всем мире электронной почты составляет спам (75 — 80%). Заметим, что распространенность данного деяния не означает, что его совершают практически все, 75 — 85% спам-рассылок отправляется по разным оценкам всего 150 — 250 спамерскими организованными группами[170].

Динамика данного явления достаточно угрожающа. Представляется, что отсутствие уголовно-правового запрета является весомым фактором в безнаказанности спамеров и в усилении возможностей их группировок. По данным экономического журнала Forbes, спамеры всего мира зарабатывают примерно 10 — 15 млрд долл. США в год; более точную оценку дать сложно, так как спамеры предпочитают скрываться из-за негативного общественного отношения к ним. Если же говорить о динамике данного явления, то в 1997 г. спам занимал около 25 — 35% всего трафика сообщений электронной почты, а в 2005 г. — уже около 75 — 80%.

Возможность воздействия на спамеров административно-правовыми мерами весьма ограниченна в силу того, что даже для установления личности спамера требуется ряд затратных действий по обнаружению, установлению, сбору доказательств и т.д., проведение которых возможно только при совершении уголовного преступления. Бесперспективно воздействие на спам техническими средствами. Во-первых, спамеры все время совершенствуют методы рассылки в обход мер защиты. И во-вторых, некоторые из методов технической защиты прямо противоречат Уголовному закону, так, например, для отсеивания спам-сообщений необходим доступ к тексту сообщения, что нарушает тайну переписки, телефонных переговоров, почтовых или иных сообщений (ст. 138 УК РФ), если прямо не заявлено о согласии лица на доступ к подобной информации. Представляется, что большинство спамеров такого согласия не дают. Этот факт в очередной раз доказывает, что спамер более защищен уголовным законом, чем пострадавший от его действий.

---

[170] См.: cnews.ru/news/top/index.shtml?2006/11/16/217442; www.viruslist.com/ru/spam/info?chapter=156614514

К сожалению, ограниченны *возможности уголовной юстиции*, хотя ввод уголовного запрета можно было бы и воспринимать как социальный заказ тех, кто в первую очередь страдает от спама, т.е. обычных пользователей глобальной сети, которые вынуждены нести дополнительные финансовые затраты в виде оплаты за услуги Интернет в связи с получением ненужной для них сетевой рекламы и тратить свое время на бесполезные электронные письма.

Кроме юридико-криминологических оснований, необходимо рассмотреть и социально-экономические основания криминализации нежелательной рассылки. Так, часто аргументом против запрета спама является тот факт, что спам — один из самых дешевых методов рекламы и поэтому уголовно-правовые санкции могут помешать малому бизнесу, который не имеет больших средств на рекламу. Но ведь речь идет не о запрете всего спама, а о регулировании его потока, о запрете именно нежелательной рассылки, которая осуществляется вопреки воле получателя, и рассылки, которая заведомо влечет негативные последствия. Контроль за данным видом деятельности необходим, чтобы отсылающий нес ответственность за электронные сообщения, которые он посылает. Пользователь должен иметь возможность отказаться от них, а рекламные сообщения иметь полную и достоверную информацию об отправителе.

Кроме того, в качестве негативных последствий уголовно-правового запрета можно предположить, что ограничение свободы распространения информации подорвет основы Интернет и приостановит его развитие. Представляется, что пока, наоборот, спам является одним из факторов, затормаживающих эволюцию Интернет-технологии. Таким образом, сравнивая негативные и предполагаемые положительные эффекты от криминализации спама, можно сделать вывод, что закрепление в уголовном законе санкций за спам просто необходимо для наведения порядка в данной области и дальнейшего развития Интернет.

Некоторые авторы приводят аргументы против криминализации спама. Так, Т.Л. Тропина приводит три основания некриминализации спама: данные деяния являются в глазах населения слишком обычными, совершаются слишком большим числом людей, искренне расцениваются значительной частью населения как доз-

воленное[171]. Заметим, что, согласно нашим исследованиям, большинство считает спам вредной для них информацией, более того около половины компьютерных специалистов поддерживают установление уголовной ответственности за спам. Также нельзя сказать, что данные деяния совершаются большим количеством людей, так как за основную часть рассылаемого в мире спама отвечает всего 150 — 200 спамерских групп. Можно провести параллель с экологическими преступлениями: повсеместно все наносят урон окружающей среде (бросают окурки, используют бытовые приборы), но не каждый совершает деяния действительно опасные для экологии. Так и со спамом: есть деяния, которые обладают достаточно высокой степенью общественной опасности и совершаются небольшим числом людей, вот именно эти деяния и необходимо криминализовать.

Ощущение дозволенности возникает у пользователей в силу того, что пользователь, получая одно сообщение, не может, не может представить всего размаха суммарного ущерба, наносимого данной рассылкой. Как в случае с экологическими преступлениями, где значительный ущерб наносится экосистеме, а не конкретному человеку, так и при рассылке спама весомый ущерб наносится функционированию какой либо подсети или всему Интернет, а не конкретному человеку[172].

Согласно проведенному выше анализу, нежелательная рассылка при определенных условиях содержит такие необходимые для криминализации признаки, как общественная опасность, распространенность, угрожающая динамика и т.д. Под определенными условиями подразумеваются степень и характер общественной опасности отдельной рассылки, что включает в себя не только количественное, но и качественное выражение. Достаточно общественно опасной является не только рассылка, причинившая значительный ущерб, но и рассылка, не наносящая значительный ущерб, но совершаемая вопреки воле пользователя, выраженной в действиях. Следовательно, рассылка должна подразумевать воз-

---

[171] Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук: 12.00.08. — Владивосток, 2005. — С. 207.

[172] Крашенинников Д.А., Последствия экологических преступлений (понятие, виды, общая характеристика) ... канд. юрид. наук: 12.00.08. — Казань, 2007. — С. 17 — 20.

можность выражения воли получателя, то есть содержать корректный обратный адрес, а также обязательно должны быть выделены средства на обработку отказа от рассылки, чтобы исключить ситуацию, при которой недобросовестный рассыльщик может указать обратный адрес электронной почты, но не просматривать сообщения, приходящие на него. Необходимость указания реквизитов отправителя и обеспечения получателю возможности отказа прописана в ст. 10 ФЗ «Об информации, информационных технологиях и защите информации» от 9 августа 2006 г.

Хотя есть предложения криминализации только рассылки, которая нанесла значительный материальный ущерб, спам вопреки воле получателя также достаточно общественно опасен. Например, отсылка 500 сообщений на один электронный почтовый ящик не несет в себе значительных материальных затрат порядка (10 рублей) при объеме сообщения в 10 Кбайт и тарифах, установленных компанией «Приморье он-лайн», но, если учесть, что пользователь суммарно в течение получаса не мог пользоваться Интернет (из-за полной загрузки трафика), а также, что он неоднократно писал отказы на получение данной информации, то отсутствие достаточной степени общественной опасности уже не так очевидно. В данном случае спамер наносит, прежде всего, моральный ущерб, демонстрируя полное пренебрежение к правам других людей. Пользователь морально истязаем назойливой информацией, согласия на получение которой он не давал. Разделяя мнение, что за спам в первую очередь должна быть административно-правовая ответственность, считаем, что наиболее опасные его формы, обладающие достаточной степенью общественной опасности, должны быть криминализованы. При этом под опасными формами подразумеваются не только деяния, причинившие существенный материальный ущерб, но и деяния, причинившие моральный вред.

Представляется, что посылка уведомления о нежелании получать почту от данного адресата должна быть легко выполнимой (не обременительной) материально и технически. Например, посылка уведомления не может требовать финансовых затрат больших, чем стоимость посылки электронного письма. Технические сложности могут быть созданы путем предложения обязательного заполнения, например, многостраничного бланка отказа.

В порядке de lege ferenda предлагаем нашу модель ст. 274^1 и ст. 274^2 Главы 28 УК РФ в следующей редакции:

Статья 274[1]. Рассылка компьютерной информации, наносящая ущерб

1. Рассылка компьютерной информации, если это деяние причинило значительный ущерб, —

наказывается ... с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до ... лет или без него.

2. Те же деяния, совершенные группой лиц по предварительному сговору, а также организованной группой, —

наказываются ... с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до ... лет.

Статья 274[2]. Рассылка компьютерной информации вопреки воле получателя

1. Рассылка компьютерной информации вопреки воле получателя, выраженной в конкретном действии, а также непредоставление возможности выражения данной воли, —

наказываются ... с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до ... лет или без него.

2. Те же деяния, совершенные неоднократно, либо совершенные группой лиц по предварительному сговору, а также организованной группой, —

наказываются ... с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до ... лет или без него.

Примечание. Условия для выражения своей воли «не получать электронные сообщения» должны быть легко выполнимы материально и физически.

Представляется, что данные статьи могли бы оказать существенное воздействие на спамеров и заказчиков подобной рекламы. Можно сказать, что пугающая динамика и организованность спам-группировок уже давно вышли из под контроля. Спамеры не боятся ни корпораций безопасности, ни правоохранительных органов. Во многом это связано с отсутствием запрета, закрепленного УК РФ. Хотя есть трудности, связанные с возможностями правоохранительных органов и реализацией уголовно-правовых мер, необходимость введения таких мер велика.

2.3. Личность Интернет-преступника

Попытки выделить преступников среди остальных людей, не совершающих преступления, учеными юристами осуществляются давно. Преступники классифицируются с учетом нравственно-психологических и социально-демографических признаков. Исследователи определяют зависимость между личностными характеристиками и видами совершаемых преступлений. При этом измеряются и фиксируются не только детали, относящиеся к моменту совершения преступления, но также аспекты, которые относятся к жизни преступника до и после преступления. Например, еще в 19 веке всемирно известный криминолог Габриэль де Тард приводит данные о том, что читают преступники, отбывающие наказание в тюрьмах. Оказалось, что самыми популярными являются романы Дюма[173].

Современному криминологу для установления причин преступности необходимо знать не только читательские предпочтения преступника, но и что он смотрит, чем увлекается, в какой среде формируются его взгляды. Для прогнозирования преступности и профилактики преступлений важно установить корреляции между факторами, воздействующими на личность, и вероятностью преступного поведения. Известно, что поведение человека детерминируется несколькими видами обстоятельств: общественной средой, непосредственным окружением, внутренним миром самого человека. Основным уровнем, определяющим поведение личности, является макросоциальный уровень, так как именно в рамках общей социальной среды устанавливаются правовые, материальные, культурные, нравственные и иные отношения, которые влияют на личность как непосредственно (например, через средства массовой информации), так и опосредованно — через воздействие на нее ближайшего окружения. Несмотря на это причины антиобщественного поведения в определенной мере могут быть заложены как в ближайшем окружении человека, так и в особенностях его личностных характеристик.

---

[173] Тард Г. Преступник и преступление. Сравнительная преступность. Преступления толпы / сост. и предисл. В.С. Овчинского. — М.: ИНФРА-М, 2004. — С. 47.

Так, по мнению В.Н. Кудрявцева, характер и нравственное формирование личности играют главную роль в генезисе преступного поведения. Не биологические свойства человека, не кратковременное и подчас случайное воздействие внешней ситуации, а весь жизненный путь индивидуума в конечном счете определяет содержание подавляющего большинства его поступков[174].

В криминологической литературе можно найти достаточно классификаций личности преступника в зависимости от признаков, характеристик, установок, видов совершенного преступления, роли в преступной деятельности и т. д.[175] При этом убийцы, мошенники, наркопреступники, фальшивомонетчики имеют свои особенности внутреннего мира, отличительные признаки характеристики их личности.

История такого молодого явления, как Интернет-преступность в России, измеряется примерно двумя десятками лет (скорее даже одним десятком, ранее только единичные преступления). Хотя и существуют отдельные исследования личности компьютерного преступника в общем и Интернет-преступника — в частности, они либо не полные[176], либо устарели в связи с быстрым изменением характеристики показателей состояния и структуры Интернет-преступности. Так, например, если научная работа основывается на данных до 2001 г., когда число преступлений в сфере компьютерной информации измерялось в пределах всего 2 000 деяний в год, то за последние 5 лет отмечено почти пятикратное увеличение (око-

---

[174] Кудрявцев В.Н. Причинность в криминологии (О структуре индивидуального преступного поведения). — М.: Изд-во «Юрид. лит.», 1968. — С. 22—23.

[175] См: Криминология: учебник для студентов вузов / Под науч. ред. Н.Ф. Кузнецовой, В.В. Лунеева. — М.: Изд-во Волтерс Клувер, 2005. — С. 119—135; Криминология: Учебник / Под ред. В.Н. Кудрявцева, В.Е. Эминова. — 2-е изд. — М.: Юристъ, 1999. — С. 124—158; Криминология. Серия «Учебники учебные пособия» / Под общ. ред. Ю.Ф. Кваши. — Ростов-на-дону:Феникс, 2002. — С. 105—119; Криминология: Учебник для вузов / Под общ. ред. А.И. Долговой. — 2-е изд. — М., 2003. — С. 326—363; Криминология: Учебник / Под ред. В.Н. Бурлакова, Н.М. Кропачева. — СПб.: Санкт-Петербурский государственный университет, Питер, 2002. — С. 64—83.

[176] Кесареева Т.П. Криминологическая характеристика и предупреждение преступности в Российском сегменте сети Интернет: дис. ... канд. юрид. наук: 12.00.08. — М., 2002. — С. 101—112.; Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение: дис. ... канд. юрид. наук: 12.00.08. — М., 2003. — С. 55—70.

ло 9 000 преступлений — в 2006 г., около 7000 — в 2007)[177]. Кроме того, многие исследования носят локальный характер и затрагивают, как правило, только отдельные центральные области РФ.

Нами было проведено исследование материалов 137 уголовных дел за 2002—2006 гг. (144 лица — всего за этот период в ДФО около 400 лиц) о преступлениях, предусмотренных ст. 272 УК РФ по Приморскому и Хабаровскому краям и Камчатской области, совершенных посредством Интернет, и были получены данные о личности преступника.

Наряду с исследованием социально-демографических признаков личности преступника, таких как пол, возраст, наличие судимостей, исследовались нравственно-психологические характеристики, мотивация, установки на посещение сайтов определенной направленности в Интернет, отношение к совершенному деянию, среда проживания.

Не все из изученных нами уголовных дел содержали подробные сведения о характеристике личности, его окружении, о результатах технической экспертизы и т. д., поэтому для выяснения мотивации и принадлежности к субкультуре хакеров и некоторых специфичных для подобных преступлений характеристик использовалось только 44 уголовных дела (48 лиц) с наиболее подробной информацией.

Наши исследования показывают, что подавляющее большинство преступников — мужчины. Из 144 выявленных в ходе расследования лиц, 97,2% — мужчин и лишь 2,8% женщин, что близко к результатам исследования, проведенного Т.П. Кесаревой в 2001 г. (мужчины — 98,2%, женщины — 1,8%)[178]. Соотношение же между полами среди пользователей Интернет в России 54% — мужчины и 46% — женщины. За рубежом, например, в США: 51% пользователей Интернет — это мужчины и 49% — женщины[179]. Это говорит

---

[177] Состояние преступности в Российской Федерации за январь — декабрь 2005 г. [Электронный ресурс]/ Официальный сайт МВД России. — Режим доступа: http://www.mvdinform.ru/index.php?docid=3998

[178] Кесареева Т.П. Криминологическая характеристика и предупреждение преступности в Российском сегменте сети Интернет: дис. ... канд. юрид. наук: 12.00.08. — М., 2002. — С. 103.

[179] Портрет российского интернетчика [Электронный ресурс] / Исследовательский холдинг ROMIR monitoring. — Режим доступа: http://www.rmh.ru/news/res_results/148.html

о большей склонности мужчин к совершению преступлений подобного рода. Наблюдается временная стабильность данного показателя, так как цифры близки к проводимому до нас исследованию и в динамике за 7 лет (1999 — 2006) изменений по полу не произошло.

По данным проведенного нами исследования, распределение преступников по возрасту выглядит следующим образом: до 18 лет — 29,9%; от 18 до 24 лет — 60,4%; старше 24 лет — 9,7%. При этом самому младшему было 12 лет, самому старшему — 45. Средний возраст преступника около 20-ти лет. Если сравнивать с исследованиями Т.П. Кесаревой, то доля преступников группы от 18 до 24 практически не изменилась (65,8%), зато процент преступников, не достигших 18 лет, заметно вырос (12,8% у Т.П. Кесаревой)[180]. Характерно, что среди совершеннолетних преступников группа от 18 до 24 лет является большинством (90,3%), хотя их доля среди Интернет-пользователей, достигших 18 лет, всего 35%[181]. Число преступников, не достигших 18 лет, может еще вырасти, так как быстрое развитие Интернет приводит к тому, что люди любого возраста и различных физических возможностей могут совершать серьезные преступления, не выходя из дома. К тому же у подростков наблюдается более низкая правовая культура и общий правовой «дефицит»[182]. Представляется, что это явление связано, прежде всего, с отсутствием системы воспитания правосознания в области компьютерной информации.

Если же сравнивать полученные данные с результатами прошлых лет, то Интернет-преступность сильно помолодела. Так, по

---

[180] Кесареева Т.П. Криминологическая характеристика и предупреждение преступности в Российском сегменте сети Интернет: дис. ... канд. юрид. наук: 12.00.08. — М., 2002. — С. 103.

[181] Портрет российского интернетчика [Электронный ресурс] / Исследовательский холдинг ROMIR monitoring. — Режим доступа: http://www.rmh.ru/news/res_results/148.html

[182] It's Not Just Fun and «War Games» — Juveniles and Computer Crime [Электронный ресурс]/ Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice. — Режим доступа: http://www.cybercrime.gov/usamay2001_7.htm; Меркурьев А.В. Социолого-криминологические аспекты борьбы с преступлениями в сфере компьютерной информации / А.В. Меркурьев, С.С. Наумов // Вестник Дальневосточного юридического института МВД России. — 2002. — № 2 (3) — С. 73 — 74.

исследованиям 2001 г. доля лиц, не достигших 18 лет, составляла 12,8%, а по данным нашего исследования 2005 г. — 29,9%. По нашему мнению, данный процент будет расти и дальше, так как увеличивается доля подростков в аудитории российского Интернет. Доля преступников от 18 до 24 лет достигает двух третей среди всех исследуемых. Это указывает на необходимость разработки мер профилактики в вопросе высокотехнологичных преступлений, в первую очередь — среди молодежи и подростков.

Постоянное место работы, по данным нашего исследования, имеют 31,3% (33% у Т.П. Кесаревой), лишь у 13,9% из выявленных лиц работа связана с обслуживанием компьютеров, программированием и т.д. Обучаются в высших учебных заведениях 38,2% респондентов, 25,7% — на технических специальностях, так или иначе связанных с компьютером; 14,6% — подростки, обучающиеся в школах. Проживает с родителями — 79,86%, и 93,06% деяний были совершены с домашнего компьютера. Это свидетельствует о том, что раскрываются наиболее простые и менее общественно опасные деяния[183].

Согласно нашим данным, все 100% лиц ранее не судимы и совершили преступление впервые. Для выяснения антиобщественной направленности личности и соблюдения уголовно-правовых запретов был проведен анализ отношения лица к содеянному и наступившим уголовно-правовым последствиям. По нашим данным, 84,72% исследуемых лиц признало свою вину и раскаялось, все из них возместили материальный ущерб. 13,19% лиц, совершивших Интернет-преступления, признали вину частично; 2,08% отрицали вину, но никто не отрицал свою причастность к преступлению. Из 48 случаев, когда к уголовному делу прилагались технические экспертизы, в 16,6% случаев была попытка удалить файлы, относящиеся к совершению преступления, мотивом удаления, скорее всего, была попытка сокрытия доказательств. В 68,8% улики скрыты не были, и в 14,6% случаев таких сведений в материалах уголовных дел не имелось.

---

[183] Принцип — не совершать, находясь у себя дома, так как очень легко попасть в руки правосудия, зафиксирован как способ ухода от уголовной ответственности во многих хакерских книгах, журналах и художественных фильмах, то есть об этом должен знать любой профессиональный Интернет-преступник.

Информация о том, состоял ли преступник на учете в наркологическом или психоневрологическом диспансере, имелась в отношения 139 лиц (96,53%), никто из них на учете ни в одном из диспансеров не состоял.

Внутренней побудительной причиной любого противоправного поведения человека является мотивация. Определенный интерес представляет анализ мотивов, которые обусловили, способствовали, предопределили или подтолкнули лицо в целях удовлетворения своих потребностей избрать преступный путь. Завышенные амбиции и потребности могут вступить в противоречие с его способностями. Верно и обратное, огромные познания техники и возможности легкого достижения целей могут не соответствовать низкому социальному статусу. В 95,83% случаев в результате противоправных деяний была получена возможность пользоваться Интернет за чужой счет, то есть налицо корыстный мотив.

Данный мотив является преобладающим в преступлениях, зарегистрированных в других регионах и за рубежом, что подтверждается в некоторых работах[184]. Например, К.Н. Евдокимов в ходе изучения уголовных дел по ст. 272 УК РФ в Иркутской области (анализировались не только преступления, совершенные посредством Интернет, но и осуществленные без использования сети) установил, что в 100% случаев имеет место корыстный мотив[185]. Корыстный мотив, как известно, является наиболее распространенным среди всех регистрируемых преступлений[186].

В ходе проведенного нами исследования было выделено несколько основных групп мотивов, которые характерны для преступников, незаконно получающих доступ к компьютерным данным. Мы располагаем их в порядке убывания:

---

[184] Осипенко А.Л. Борьба с преступностью в компьютерных сетях: Международный опыт: Монография. — М.: Норма, 2004. — С. 165—166; Shinder D.L. Scene of the cybercrime: computer forensics handbook. — Syngress Publishing. Inc., 2003. — P. 113—144.

[185] Евдокимов К.Н. Уголовно-правовые и криминологические аспекты противодействия неправомерному доступу к компьютерной информации: дис. ... канд. юрид. наук: 12.00.08. ? Иркутск, 2006. — С. 146. См. также: Старостина Е.В. Защита от компьютерных преступлений и кибертерроризма / Е.В Старостина, Д.Б. Фролов. — М.: Изд-во Эксмо, 2005. — С. 27.

[186] Долгова А.И. Преступность в России начала XXI века и реагирование на нее / А.И. Долгова и коллектив авторов; Под ред. профессора А.И. Долговой. — М.: Российская криминологическая ассоциация, 2004. — С.14.

1) корыстные побуждения — 95,83%;

2) любопытство и исследовательские побуждения — 58,33%;

3) доказательство собственного превосходства — 22,92%;

4) желание приобщиться к популярной хакерской субкультуре — не ниже 18,75%.

Представляется, что доля некорыстных мотивов может быть и выше, так как материалы уголовного дела не позволяют зачастую точно установить мотив. На первый взгляд, материальная заинтересованность является самым распространенным стимулом для совершения исследованных преступлений, однако есть объективные предпосылки, что это не так. Средний размер ущерба в данных случаях составлял около 520 рублей. Примеров того, что преступник живет в неблагополучной среде (семья алкоголиков, бедная или асоциальная) не зафиксировано. Многие из допрошенных родителей показали, что для них не было затруднительно оплачивать услуги Интернет. Если большинство из лиц, совершивших Интернет-преступления, не испытывало финансовых трудностей в легальной оплате Интернет, то корыстный мотив сопровождался другими внутренними побуждениями, такими как любопытство и тяга к исследованиям; доказательство собственного интеллектуального превосходства, желание приобщиться к популярному течению.

Во многих уголовных делах (в 58,33% случаев) присутствуют свидетельства того, что мотивами противоправного деяния являлись: любопытство, стремление совершить личное открытие, побуждения исследовать неизвестное и т.д. Например, один из подозреваемых показал, что он посетил сайт MazaFaka.ru (на англ. — нецензурное выражение), где узнал о программе «Троянский конь». Данная программа позволяла скачивать информацию с чужих компьютеров. Ему стало интересно, действительно ли это так, и он воспользовался данным вредоносным программным обеспечением[187]. Это созвучно со словами знаменитого «хакера», известного под псевдонимом Mentor: «Да. Я преступник. Мое преступление — любопытство (пытливость)»[188].

---

[187] Уголовное дело № 508922/03 Следственный отдел при ОВД Первореченского района г. Владивостока.

[188] Mentor. Hacker Manifesto [Электронный ресурс] // project «Cyberpunk». — Режим доступа: http://project.cyberpunk.ru/idb/hacker_manifesto.html; «Yes. I am offender. My crime is curiosity»

Более чем в каждом пятом изученном уголовном деле (22,92%) усматривается мотив доказательства собственного интеллектуального превосходства и личных способностей. Так, обвиняемый В. сказал, что он взломал компьютер потерпевшего, потому что тот никак не защищал свои данные, и если бы жертва преступления хоть чуть-чуть разбиралась в компьютерах, то преступление было бы невозможно, так как использовались стандартные общедоступные функции операционной системы[189]. Около 8% родителей, чьи дети были привлечены к уголовной ответственности, предупреждали их об осторожности в компьютерных «проделках», но те отмахивались, указывая родителям на их некомпетентность.

Почти каждый пятый из числа исследуемых лиц (18,75%) заявлял, что подобного рода преступления совершают многие, об этом они слышали в Интернет-чатах[190], в Интернет-досках объявлений или читали на «хакерских» порталах. Нет свидетельств, считают ли другие преступники, что так делают все, но они тоже сталкивались с информацией, пропагандирующей Интернет-преступления, так как в 66,67% случаев средства для совершения преступлений были взяты непосредственно в Интернет с «хакерских» сайтов. Известно, что многие сайты, на которых размещены программы для компьютерного взлома, чтения чужой электронной почты, уничтожения улик, содержат методические рекомендации и информацию идеологической направленности. Например, Crackzone (англ. — «зона взлома») не только распространяет программы, необходимые для совершения Интернет-преступлений, но и содержит информацию об известных компьютерных взломщиках, а также подробно рассказывает о том, как были совершены и какими средствами те или иные взломы[191].

На многих преступников повлияла так называемая субкультура «хакеров». Идеология и пропаганда того, что Интернет-преступ-

---

[189] Уголовное дело № 545822/03. Следственный отдел при ОВД Первореченского района г. Владивостока.

[190] Чат — сайт, позволяющий в реальном времени обмениваться текстовыми сообщениями и файлами.

[191] http://crackzone.nm.ru/; Раздел downloads [Электронный документ] / CRACKZONE. — Режим доступа: http://crackzone.nm.ru/download/program_xak/index.htm; Раздел Хакеры [Электронный документ] / CRACKZONE. — Режим доступа: http://crackzone.nm.ru/doc/xaker/index.htm

ления являются нормой для современного человека, послужили дополнительным мотивом для противоправного поведения. При этом не обязательно явное одобрение преступности. Ряд ученых доказал, что члены определенных субкультурных групп имеют личностные ценности, влекущие за собой совершение преступлений, но в явном виде не одобряют преступления[192].

Хотя основным мотивом является корыстный, декларируемая философия «хакеров» не поддерживает заинтересованность в деньгах. В идеологии «хакерской» субкультуры одним из основных положений является борьба с обществом потребления. При этом утверждается, что цены на такие услуги, как Интернет и телефонная связь, сильно завышены и поэтому бесплатное их использование одобряется. Пропагандируется хакерами и свобода доступа к информации. А ведь большинство противоправных деяний в сфере компьютерной информации — это незаконный доступ к информации. Таким образом, рассматривая личность преступника, нельзя не отметить влияния на него хакерской субкультуры. При этом желание приобщения к этому субкультурному образованию является подчас одним из ключевых мотивов.

Подводя итоги исследования личности преступника, совершившего неправомерный доступ к компьютерной информации (ст. 272 УК РФ), можно описать его характерный социальный портрет: это в основной своей массе мужчина, который имеет асоциальные установки, реже — общественно опасные. Он не состоит на учете в психоневрологическом и наркологическом диспансере, не судим, хорошо разбирается в компьютерных технологиях. Преступник молод и зачастую материально зависим от родителей или других родственников, как правило, с ними и живет, совершая преступления, как говорится, не выходя из дома. Не задумываясь об ответственности, он не пытается скрыть следы преступления и разделяет некоторые ценности субкультуры хакеров. В большинстве случаев присутствует корыстный мотив. После того, как преступление было раскрыто, он признает свою вину и, как правило, раскаивается в содеянном.

Вряд ли данных преступников можно назвать профессиональными. Они не уничтожают улики и совершают достаточно простые

---

[192] Криминология / под. ред. Дж. Ф. Шели / пер. с англ. — СПб.: Питер, 2003. — С. 419.

в техническом плане преступления. При этом для совершения противоправных деяний используются чаще всего средства, созданные другими людьми, полученные посредством Интернет. Это подтверждает предположение о том, что Интернет-преступность высоколатентна, а особо опасные, технически квалифицированные преступники остаются безнаказанными. С этой мыслью согласны и некоторые авторы, утверждающие, что не выявленными остаются самые организованные и опасные преступления в силу ограниченных возможностей правоохранительных органов[193].

Все преступники могли бы остаться безнаказанными, если бы не пользовались паролями, полученными в результате незаконного доступа к компьютерной информации. Нет ни одного случая обращения потерпевшего, уличившего непосредственно незаконный доступ, а не использование Интернет за его счет, поэтому сложно говорить о корыстной мотивации как о приоритетной. Ведь при отсутствии корыстного мотива сложно обнаружить факт незаконного доступа, и преступления без корыстного мотива остаются за пределами внимания правоохранительных органов и исследователей, что лишний раз подтверждает высокую латентность Интернет-преступлений.

В силу того, что Интернет-преступность неоднородна, нельзя составить обобщенный портрет Интернет-преступника. Скорее следует говорить об Интернет-мошеннике, Интернет-взломщике, создателе Интернет-вирусов как о субъектах, имеющих различные характеристики личности. Из-за высокой латентности и малого количества уголовных дел по Интернет-преступлениям по статьям УК РФ (например, ст. 242 УК РФ, ст. 159 УК РФ и т.д.), кроме ст. 272 УК РФ, мы получили подробный портрет только личности, осуществившей неправомерный доступ. Представляется, что кроме ст. 272 УК РФ существуют и другие виды правонарушений: распространение вредоносных программ (ст. 273 УК РФ), экономические преступления посредством Интернет, распространение порнографии и др. При этом мотивы, социальное положение, нравственные установки и другие характеристики личности преступников в этих сферах могут различаться.

---

[193] Колмыков В.В. Криминологическая характеристика компьютерных преступлений // Вестник Дальневосточного юридического института МВД России. — 2005. — № 1(8) — С. 84—87.

Несмотря на то, что разработчики вирусов также могут нарушать и ст. 272 УК РФ, но все же создатели вредоносных программ отличаются от остальных Интернет-преступников. Как правило, они объединены в собственные сообщества в Глобальной сети («29A», «SMF», «Duke Legion», «SL»); имеют свои периодические издания вне России[194]. Создатели вирусов встречаются и обмениваются мнениями на специализированных сайтах в Интернет[195].

Представляется, что вирусы — это целый класс компьютерных программ, имеющих разное назначение и реализацию. Не все компьютерные вирусы умышленно деструктивны: есть вирусы, борющиеся с другими вирусами или, например, с детской порнографией. По воздействию на компьютерную систему предлагаем разделить их на несколько видов: поражающие всю систему; поражающие отдельные функции системы; затрудняющие работу системы; нейтральные; позитивно ориентированные.

Создатели и распространители первых трех категорий вирусов — это зачастую асоциально настроенные личности, пытающиеся добиться признания. Характерное их отличие от специалистов незаконного доступа в том, что прирожденные вирусописатели не стремятся остаться незамеченными, наоборот, каждый создатель деструктивного вируса стремиться, чтобы его заражающая программа распространилась как можно шире и была известна большему числу лиц. Поэтому в коде вируса часто хранится имя группы вирусописателей или псевдоним преступника, если он действовал самостоятельно.

В своих сообществах писатели вирусов могут стать знаменитостями и получить в СМИ скандальную репутацию как создатели известных и распространенных вирусов. Чтобы добиться успеха в своем деле, они должны уметь ярко и эффективно программировать. Если писатель вирусов создал наиболее совершенный вирус и заразил больше всех систем, то он пользуется наибольшим уважением среди своих коллег[196].

---

[194] («DVL» — Duke's Virus Labs: рус. — «Вирусные лаборатории Дюка»; «Infected voice»: рус. — «Инфицированный глас»; «VLAD» — Virus Labs and Distribution: рус. — Вирусные лаборатории и распространение; «MoonBug»: рус. — «Ошибка в программировании определенного вида» и т. д.)

[195] «smf.chat.ru», «computervirus.meetup.com», «subseven.slak.org» и др.

[196] Уорли Б. Интернет: реальные и мнимые угрозы / Пер. с англ. — М.: КУДИЦ-ОБРАЗ, 2004. — С. 114.

По мнению Е.В. Касперского, причина, заставляющая вирусописателей направлять свои способности на такую бессмысленную работу, — это комплекс неполноценности. Только программистов, которые пишут вирусы не для распространения, а для исследования, Е.В. Касперский выделяет в отдельную группу, указывая, что они создают вирусы совсем по другим мотивам[197]. Они занимаются разработкой и программированием вирусов из исследовательских побуждений, не ради деструктивного потенциала, а для исследования самих возможностей компьютерных технологий.

Даже при отсутствии деструктивной мотивации опасность от вирусописания не снижается, так как идеи и решения из подобных вредоносных программ быстро заимствуются другими компьютерными преступниками. Хотя данная группа создателей вирусов может и не запускать свои творения в жизнь, однако очень активно пропагандирует свои идеи через многочисленные сайты, журналы.

Представляется, что портрет личности вирусописателя сильно отличается от характеристик типичного преступника, осуществляющего неправомерный доступ. Компьютерные взломщики менее склонны к популярности, чем вирусописатели, они зачастую скрывают свои преступления и даже псевдонимы. Кроме того, за неправомерным доступом в отличие от намерений создателей вирусов, чаще стоит корыстный мотив.

Дальнейшие исследования личности Интернет-преступника позволят более ясно понять причины стремительного роста Интернет-преступности, проследить ее тенденции и динамику, научиться прогнозировать появление новых видов в ее структуре, а также разработать профилактические меры среди молодежи и подростков с целью воспитания правовой культуры поведения в Интернет, восполнения правового дефицита и нейтрализации негативных воздействий субкультуры хакеров, способствующих росту Интернет-преступности.

---

[197] Касперский Е.В. Компьютерные вирусы: что это такое и как с ними бороться. — М.: СК Пресс, 1998. — С. 17.

2.4. Виктимологические проблемы Интернет-преступности

Личность и поведение потерпевшего могут играть существенную роль в мотивации преступного поведения и создании ситуации, в которой такое поведение становится возможным. Виктимность — это способность лица по разным основаниям становиться жертвой преступлений. Источником такой способности могут являться: состояние (например, опьянение, усталость); физические особенности (нарушение опорно-двигательных функций или дефекты органов чувств); психические отклонения. Определенные действия и поведение в целом могут также быть основой для виктимности.

На способность стать жертвой преступления влияет несоблюдение элементарных, известных потерпевшему правил безопасности, либо незнание таких правил. Большинство правил не закреплено законом и нередко носит бытовой характер. Например, чтобы снизить вероятность стать потерпевшим от кражи, лучше не оставлять вещи без присмотра.

Криминологами уже давно проанализированы зависимости между личностью, состоянием, поведением жертвы и вероятностью стать жертвой традиционных видов преступлений, таких как кража, убийство и т.д. История мировой Интернет-преступности пока измеряется несколькими десятилетиями, а в России и того меньше, порядка двух десятков лет. В существующих исследованиях характеристики Интернет-преступности зачастую не уделяется внимание проблеме виктимологии жертв преступлений в сети Интернет, либо в них характеризуются лишь отдельные подвиды Интернет-преступлений, не раскрывающие подробно другие виды и все явление в целом.

Так, например, Д.А. Зыков в своей диссертационной работе исследует виктимологические аспекты компьютерного мошенничества, выделяя как подвид характеристики мошенничества с использованием сети Интернет.

Автор выделяет подвиды посткриминального поведения жертвы компьютерного мошенничества и разрабатывает меры предупреждения, предлагая для более эффективной виктимологической профилактики создать Центр учета и анализа компьютерных мо-

шенничеств[198]. Интернет-мошенничество очень специфичный подвид Интернет-преступлений, и поэтому выводы, содержащиеся в диссертации, лишь отчасти применимы ко всей преступности в Глобальной сети. Интернет-мошеннику не обязательно разбираться в сетевых технологиях, а лишь достаточно знать психологию жертвы. В свою очередь, потерпевшим от мошенничества с большой вероятностью может стать и высококлассный компьютерный специалист, оснастивший свою ЭВМ системой защиты.

М.С. Гаджиев рассматривает виктимность обладателей компьютерной информации как одну из главных специфичных детерминант компьютерной преступности, выделяя виды виктимного поведения для компьютерных преступлений и предлагая меры виктимологической профилактики. При этом утверждается, что главная виктимологическая причина — это техническая неграмотность пользователей[199].

Д.А. Ястребов в своей работе находит связь между виктимологической характеристикой неправомерного доступа к компьютерной информации и ее высокой латентностью. Он рассматривает случаи умалчивания жертвами фактов компьютерных преступлений и определяет причины подобного поведения[200]. Хотя неправомерный доступ является самым распространенным в России видом Интернет-преступлений, он всего лишь один из множества подвидов преступности в Глобальной сети и сильно отличается от других видов Интернет-преступлений, например, от распространения вредоносных программ. При этом нельзя не согласиться, что виктимологическая характеристика и латентность компьютерной преступности находятся в тесной связи.

Т.П. Кесарева в своей работе, посвященной преступности в российском сегменте сети Интернет, уделяя проблеме виктимологии всего 4 стр., делит потерпевших на следующие группы: коммерческие организации; правоохранительные органы; предприятия связи

---

[198] Зыков Д.А. Виктимологические аспекты предупреждения компьютерного мошенничества: дис. ... канд. юрид. наук: 12.00.08. — Владимир, 2002. — С. 156—165.

[199] Гаджиев М.С. Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан): дис. ... канд. юрид. наук: 12.00.08. — Махачкала, 2004. — С. 81—85.

[200] Ястребов Д.А. Неправомерный доступ к компьютерной информации: уголовно-правовые и криминологические аспекты: дис. ... канд. юрид. наук: 12.00.08. — М., 2005. — С. 137—138.

и провайдеры Интернет; частные лица; магазины электронной торговли; частные банки; иностранные физические и юридические лица[201]. Данные категории потерпевших пересекаются — например, магазин электронной торговли может являться как коммерческой организацией, так и юридическим лицом; также как и предприятие связи или провайдер. Более того, в работе не объяснено, откуда получены данные о процентном соотношении этих групп.

Вышеперечисленные исследования носят фрагментарный характер в отношении виктимологической характеристики Интернет-преступности в целом. Несмотря на то, что ряд сделанных выводов применим и к проблеме потерпевших от преступлений в Глобальной сети, представляется, что данный вопрос нельзя назвать достаточно изученным.

Интернет-преступность неоднородна, и поэтому причины виктимности в зависимости от подвида деяний могут существенно различаться: неправомерный доступ к компьютерной информации (ст. 272 УК РФ) посредством использования чужих паролей доступа в Интернет; умышленное уничтожение или повреждение имущества (ст. 167 УК РФ); распространение вредоносных программ (ст. 273 УК РФ); Интернет-мошенничество (ст. 159 УК РФ), клевета (ст. 129 УК РФ) и др.

Неправомерный доступ является самым распространенным видом как Интернет-преступлений, так и преступлений в сфере компьютерной информации[202]. Согласно изученным нами материалам уголовных дел, возбужденных по ст. 272 УК РФ в 2004—2005 гг., где неправомерный доступ был осуществлен посредством Интернет, получился следующий портрет личности потерпевшего от Интернет-преступления. Мужчины становились жертвами преступлений в 54,8% случаев, а женщины — в 45,2%. Соотношение полов в российской Интернет-аудитории приблизительно такое же[203]. Средний возраст потерпевшего около 34 лет, что на 4 года

---

[201] Кесареева Т.П. Криминологическая характеристика и предупреждение преступности в Российском сегменте сети Интернет: дис. ... канд. юрид. наук: 12.00.08. — М., 2002. — С. 109—112.

[202] Шаповалова Г.М., Возможность использования информационных следов в криминалистике: автореферат на соискание степени ... канд. юрид. наук: 12.00.09. — Владивосток, 2006. — С. 3, 12.

[203] Портрет российского интернетчика [Электронный ресурс] / Исследовательский холдинг ROMIR monitoring. — Режим доступа: http://www.rmh.ru/news/res_results/148.html

больше среднего возраста пользователя Интернет в России. В 90,5% случаев потерпевшие не были знакомы с преступником, что можно объяснить спецификой совершенных преступлений. Например, программы для компьютерного взлома, которые отыскивают незащищенные компьютерные системы, подключенные в Интернет, делают это случайным образом и не персонифицированно. Злоумышленнику достаточно указать диапазон IP-адресов[204], и программа для взлома случайным образом или последовательно будет проверять на возможность неправомерного доступа все компьютеры, находящиеся в сети, адреса которых принадлежат указанному диапазону. Преступник зачастую не знает ни географического расположения системы, к которой он получает доступ, ни персоны жертвы.

Анонимность — один из главных принципов работы Интернет, поэтому жертвы, как правило, не знакомы со злоумышленником как в случае с неправомерным доступом, так и при других видах противоправных деяний в Глобальной сети. Например, при распространении вредоносных программ (вирусов, червей и т.д.), за что установлена уголовная ответственность по ст. 273 УК РФ; вирусы в основном распространяются автоматически, а каждая зараженная система самостоятельно заражает следующую, поэтому персонифицировать злоумышленника бывает достаточно сложно, так же как и злоумышленник зачастую не знает владельцев систем, которые он «заразил»[205].

В рамках проведенного нами исследования было установлено, что в 78,6% случаев пострадавшие от незаконного доступа посредством Интернет не защищали свои данные, и преступники беспрепятственно с помощью общераспространенных программ получили доступ к вычислительным машинам жертв.

Небрежность в вопросах защиты своей информации дает дополнительный стимул не только для совершения конкретного преступления, но и является обстоятельством, способствующим росту количества преступлений, совершенных посредством Интер-

---

[204] Уникальный номер, который есть у любой компьютерной системы, находящейся в сети Интернет. При этом данный номер может быть как статическим, т.е. закреплен за отдельным компьютером, так и динамическим, т. е. выделяться непосредственно при входе в сеть.

[205] Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение: дис. ... канд. юрид. наук: 12.00.08. — М., 2003. — С. 27—29.

нет[206]. Представляется, что отсутствие средств защиты компьютерной системы не только упрощает Интернет-преступления, но и психологически подкрепляет уверенность «хакера» в его безнаказанности[207].

Несмотря на то, что большинство авторов выделяет техническую неграмотность пользователя как основную причину виктимности, осуществление Интернет-преступления не ограничивается только использованием узкотехнических приемов. Например, компьютерные пароли потерпевшего можно получить, представившись системным администратором сети по телефону, или создать Интернет-сайт, похожий на благотворительный, и обманом собирать деньги. Подобные способы совершения компьютерных и Интернет-преступлений, где преступная цель достигается не с помощью технических приспособлений или компьютерных программ, а с помощью обмана, иногда при непосредственном контакте с потерпевшим, объединены в группу методов, называемую «хакерами» «социальной инженерией».

Представляется, что данные методы хорошо проработаны и известны профессиональным Интернет-преступникам. Например, известный хакер Кевин Митник издал книгу Art of Intrusion (рус. — «искусство вторжения»), электронными копиями которой завален весь «хакерский» Интернет. Большая часть этой книги посвящена методам обмана и получения нужной информации не «компьютерными» способами. Сам он не раз в ходе своей преступной карьеры применял «социальную инженерию», представляясь сотрудником телефонной компании, копаясь в мусоре (для поиска информации о паролях и учетных записей). Заметим, что в отличие от технических приемов, описанных в его книгах, которые уже устарели, нетехнические методы актуальны и сейчас.

То есть для того чтобы не стать жертвой Интернет-преступления, кроме технической защиты своей компьютерной системы необходимо эффективно противостоять «взлому мозга», как иногда

---

[206] Расследование неправомерного доступа к компьютерной информации: учебное пособие / Под. ред. д.ю.н. проф. Н.Г. Шурухнова. — Изд. 2-е, перераб. и доп. — М.: Московский университет МВД России, 2004. — С. 284.

[207] Более того, преступники пренебрежительно отзываются о владельцах (в Интернет-форумах, в журналах, на хакерских сайтах) таких незащищенных систем, употребляя к ним оскорбительное в преступной среде Интернет слово «ламмер» (от англ. lamer — калека, хромой).

называют хакеры обман[208]. Наиболее распространенными нетехническими ошибками, которыми пользуются Интернет-преступники, являются: передача паролей другому лицу и покупки в незнакомых Интернет-магазинах, чем часто пользуются Интернет-мошенники.

Интернет-мошенничество — это подвид компьютерного мошенничества, в котором используется определенная компьютерная технология Интернет. Под компьютерным мошенничеством понимают завладение денежными средствами или причинение имущественного вреда путем использования банкоматов, сети Интернет, игровых автоматов, а также путем манипуляций со средствами ввода-вывода и с использованием сотовой телефонной связи[209]. По нашему мнению, главным критерием того, что это Интернет-мошенничество, является все-таки обман или злоупотребление доверием человека как способ совершения. Обман также совершается посредством Интернет, — например, поддельный Интернет-магазин, выдающий себя за настоящий; тут налицо обман как способ, но обман с использованием свойств Интернет. Заметим, что проникновение в банковскую систему и перевод денег или технический взлом автоматизированной игровой системы, не являются Интернет-мошенничеством или компьютерным мошенничеством, так как тут нет обмана, есть взлом технических защит. Ведь никому не придет в голову называть обманом взлом с помощью отмычки или проникновение через дыру в заборе, хотя дискуссий на эту тему хватит на целое научное исследование.

Как и жертвы неправомерного доступа, потерпевшие в результате компьютерного мошенничества в большинстве случаев (70,3%) не знакомы с жертвой[210] . Такие особенности Интернет, как анонимность и возможность доступа из любой точки мира, позволяют мошенникам совершать преступления в масштабах всей планеты и против граждан любой страны.

По данным Центра анализа Интернет-мошенничества (Internet Fraud Complaint Center), больше всего шансов стать жертвой обма-

---

[208] Например январский номер за 2007 год на обложке содержит следующий анонс статьи «Взламываем мозг или хакерские секреты общения»

[209] Зыков Д.А. Виктимологические аспекты предупреждения компьютерного мошенничества: дис. ... канд. юрид. наук: 12.00.08. — Владимир, 2002. — С. 45—46.

[210] См: Там же. — С. 112.

на в сети участников онлайновых аукционов: почти 43% всех случаев мошенничества, зафиксированных в последние годы, произошло именно с участниками аукционов. Каждый пятый потерпевший (18 — 22%) был обманут нечестными продавцами товаров и услуг, а около 15% инцидентов было связано с так называемыми «нигерийскими письмами» (предложениями о помощи в вывозе за пределы страны крупных денежных сумм). И только в 1,4% криминальных ситуаций виновными оказывались предприятия электронной торговли. Бизнес-структуры страдают гораздо больше, чем частные лица. Мужчины становятся жертвами подобных преступлений чаще, чем женщины, а пожилые люди чаще, чем молодые[211].

Еще один вид Интернет-преступлений, который имеет свои особенности, — это создание, использование и распространение вредоносных программ для ЭВМ. Так, по исследованиям, проведенным в Приморском крае, 100% опрошенных работников компьютерных служб и служб информационной безопасности предприятий в течение 2004 г. столкнулись с заражением их компьютера вирусом, при этом 57,2 % — неоднократно[212]. Согласно проведенному нами опросу, 100% компьютерных специалистов считают, что наиболее вероятно приобрести вирус в Интернет и через электронную почту, в том числе спам, что также относится к Интернет-технологии, то есть «заражение» посредством глобальной сети является самым часто встречающимся видом распространения вредоносных программ. Способы совершения данного вида преступлений в сети бывают как активные, когда преступник непосредственно воздействует на атакуемую систему, так и пассивные, когда создаются условия, чтобы пользователь системы самостоятельно загрузил именно себе вредоносную программу, например, под видом полезной[213].

---

[211] Виктор Сабадаш. Современное состояние проблемы распространения мошенничества в Интернете [Электронный ресурс] / Исследовательский Центр исследования компьютерной преступности Crime-Research. — Режим доступа: http://www.crime-research.ru/articles/Sabadash1204/7

[212] Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук: 12.00.08. — Владивосток, 2005. — С. 103.

[213] Соловьев Л.Н. Расследование преступлений, связанных с созданием, использованием и распространением вредоносных программ для ЭВМ: дис. ... канд. юрид. наук: 12.00.09. — М., 2003. — С. 52 — 57.

Активные способы в основном сопровождаются неправомерным доступом. То есть жертвами данных преступлений также становятся лица, не предпринимающие никаких мер по защите своих персональных систем. Пассивные способы существенно отличаются: во-первых, преступник не знает лично, кто из пользователей подвергнется воздействию вредоносной программы; во-вторых, получается, что пользователь заражает свою систему сам, хотя для этого создаются определенные условия. То есть потерпевший сам дает себя «заразить». При этом большинство вирусов, гуляющих в Интернет, — это вредоносные программы, которые были созданы достаточно давно и с которыми в настоящее время уже научились бороться. Виктимности способствует отсутствие современных антивирусных программ на компьютере, либо их полное отсутствие, а также доверчивость пользователей. Так, например, вирус Troj/Stinx-N рассылается в виде сообщений электронной почты, в которых тема письма может быть одной из следующих «CCTV still of Rapist» (Кабельное ТВ засняло насильника), «Do you recognise this person?» (Вы можете узнать этого человека) и т.д. Любой, кто запустит вложенный к электронному письму файл, подвергается риску открыть хакерам доступ на свой компьютер и позволить им шпионить, похищать информацию и производить разрушения компьютерных систем от чужого имени. То есть хакеры пытаются проникнуть на компьютер обманом или техническими ухищрениями.

Кроме того, отсутствие средств защиты и мониторинга компьютерных систем, подключенных в Интернет, делает невозможным своевременное обнаружение неправомерного доступа. Так, большинство заявлений от потерпевших в проанализированных уголовных делах поступили не сразу по факту вторжения в их компьютеры, а намного позднее. Поводом для подачи заявления о совершении преступления послужил материальный ущерб, нанесенный при использовании паролей для доступа в Интернет, полученных в результате неправомерного доступа.

В целом можно сказать, что жертвами незаконного доступа в подавляющем большинстве становятся люди, не предпринимающие никаких мер по защите своих персональных систем. Так, согласно нашим исследованиям, 73,8 % жертв не использовали технические средства по защите информации и для мониторинга незаконного проникновения. Исходя из проведенного нами анализа, пренебрежение средствами компьютерной защиты носит повсеместный ха-

рактер. То есть основным виктимологическим фактором является несоблюдение потерпевшим мер информационной безопасности, а не знакомство с преступником, антропологические характеристики или какие-либо другие факторы виктимизации.

Не сообщение в правоохранительные органы о факте преступления является одной из причин высокой латентности. Размер скрытых от официальной статистики инцидентов в России не поддается оценке. Какие же причины побуждают жертв утаивать факт Интернет-преступлений в целом и неправомерного доступа, в частности. Представляется, что в первую очередь — это нежелание потерпевшего открывать доступ в персональный или рабочий компьютер для правоохранительных органов к своим личным или деловым данным, будь это частное лицо или организация. Во-вторых, это неверие в то, что Интернет-преступник будет наказан и нежелание бесполезно тратить время на хождение в органы УВД и прокуратуры. В-третьих, боязнь того, что огласка инцидента нанесет урон репутации безопасности потерпевшего, а кроме этого привлечет других компьютерных преступников к их незащищенной и уязвимой системе. В-четвертых, общая низкая правовая культура и правосознание, особенно в вопросе Интернет. Все эти причины способствуют высокой латентности.

И наконец, к числу причин латентности можно отнести то, что значительная часть жертв не в состоянии обнаружить факт совершения преступления, так как многие из Интернет-преступлений не оставляют следов: например, неправомерный доступ без причинения материального ущерба, практически не встречается в следственной практике Приморского края.

Представляется, что нежелание потерпевших сообщать о фактах неправомерного доступа можно компенсировать, разрешив активно защищать собственные компьютерные системы, например, используя некоторые вредоносные программы против преступников. Вопрос о противодействии корыстной преступности в конкретных случаях успешно решается и при помощи негосударственных охранных структур, наделенных определенными полномочиями, и в состоянии крайней необходимости освобождаемых от уголовной ответственности за действия, внешне выглядящие как преступления.

Проблема активного противодействия преступлениям, совершаемым с помощью Интернет, уже исследовалась российскими учеными. Так, А.Е. Шарков считает, что противодействовать терроризму

следует при помощи неправомерного доступа органов безопасности к сайтам и системам ЭВМ террористических организаций со ссылкой на то, что этот случай относится к обстоятельствам крайней необходимости[214]. Возможность отвечать хакерам какими-либо активными мерами, — например, вредоносными программами или незаконным доступом, уже давно используется правительством США. Так, некоторые улики против хакеров добываются их же методами[215].

Представляется, что использование специфического программного обеспечения, поражающего компьютерную систему злоумышленника при попытке нелегального проникновения в систему, или программного обеспечения, позволяющего обнаружить преступника при помощи неправомерного доступа к его системе, обосновано крайней необходимостью. Результаты нашего исследования подтверждают необходимость разработки и внедрения системы виктимологической профилактики Интернет-преступлений. Во-первых, важно создать систему мер правовой пропаганды и повышения уровня правосознания. Во-вторых, выстроить эффективную криминологическую профилактику, направленную на повышение технического уровня пользователей с учетом соответствующей аудитории: Интернет-пользователей, которые не используют средства защиты или не знают о существовании таковых, и профессиональных пользователей, которым необходимо получать информацию о новых внедрениях в сфере компьютерной безопасности. Рекомендуемые средства защиты должны ранжироваться в зависимости от ценности защищаемых компьютерных данных и навыков пользователя.

---

[214] Шарков А.Е. Неправомерный доступ компьютерной информации: преступность деяния и проблемы квалификации: дис. ... канд. юрид. наук: 12.00.08. — Ставрополь, 2004. — С. 123—128.

[215] Андрей Анненков. Прорехи в сети [Электронный ресурс] / Информационный портал RAMBLER. — Режим доступа: http://www.rambler.ru/db/press/msg.html?s=260000271&mid=7756552

Глава 3. Особенности детерминации, предупреждения и борьбы с Интернет-преступностью

3.1. Криминологическое исследование общественного мнения о современном состоянии Интернет-преступности

Основным принципом правового государства является обоюдная ответственность государства и общества, то есть социум не только может выражать свое коллективное мнение, но и государству для легитимности своей власти следует руководствоваться общепринятыми ценностями. Это позволяет избежать обособления государства от народа и, как следствие, произвола по отношению к народу.

Несмотря на важность проблемы Интернет-преступности для современного общества, до сих пор не проводилось достаточных научных исследований общественного мнения о преступности в Глобальной сети, заполненности сети как преступной информацией, так и информацией, способствующей росту преступности. В связи с быстрым развитием Глобальной сети многие исследования теряют со временем свою актуальность, что требует систематического изучения новых характеристик, тенденций, изменений и т.д. Установлено, что на рост преступности в сфере компьютерной информации, на изменение ее форм влияют не только существующая социальная среда, но и формирующаяся социальная среда виртуального пространства[216].

В рамках проведенного нами исследования по специально разработанной анкете были опрошены две группы пользователей Интернет и одна группа, не знакомая с Интернет: первая — профессиональные компьютерщики (программисты, системные администраторы, студенты компьютерных специальностей — всего

[216] Кашапов Р.М., Наумов С.С. Проблемы с распространением детской порнографии в глобальной сети Интернет // Вестник Дальневосточного юридического института МВД России. — 2004. — № 2. — С. 72.

127 чел.), которые выделены как группа «Профессионалы»; вторая — использующие Интернет часто, но не имеющие специального компьютерного образования (группа «Гуманитарии» — 149 чел.); третья — группа людей, которые не пользуются Интернет и не умеют с ним работать (87 чел.).

Как выяснилось, и «Профессионалы», и «Гуманитарии» часто сталкиваются в Интернет с информацией, которой, по мнению подавляющего большинства, не должно быть в свободном доступе (сведения о наркотиках, порнографическая продукция и т.п.). Первая группа в 93,94% случаев и вторая — в 89,65%.

Первым вопросом был: «Какую информацию, распространяемую в Интернет, вы считаете вредной». Результаты представлены в таблице 16.

Таблица 16

Вопрос: Какую информацию, распространяемую в Интернет, вы считаете вредной?
(Возможно несколько вариантов ответов)

Вид информации	Профессионалы	Гуманитарии	Не пользующиеся Интернет
Информация, позволяющая изготовить в домашних условиях взрывчатые вещества и взрывные устройства	51,18%	75,83%	75,86%
Информация, позволяющая изготовить в домашних условиях наркотические вещества	88,19%	79,19%	90,8%
Порнографическая продукция с участием детей	96,85%	89,93%	95,4%
Порнографическая продукция, доступная для просмотра детям и несовершеннолетним	81,89%	69,13%	80,46%
Информация, призывающая к расовой и межнациональной конфронтации	66,93%	75,84%	62,07%
Информация о том, как совершать компьютерные преступления и с помощью каких средств	24,41%	48,32%	37,93%
Иная	6,3%	3,36%	0%

Полученные результаты показывают, что «компьютерщики» склонны считать информацию о том, как совершать компьютерные преступления, менее вредной, чем другие виды негативной

информации. Возможно, это вызвано тем, что «компьютерные специалисты» используют данную информацию прежде всего для профессиональных непреступных целей, — например, для эффективной защиты от взлома. Или они симпатизируют компьютерным преступникам, считая подобное противозаконное поведение допустимым.

Необъяснима также, на первый взгляд, их благосклонность к информации, позволяющей в домашних условиях изготовить взрывчатые вещества. Для обоснования этого факта надо обратиться к выпускам журнала «Хакер», в котором часто публикуют статьи об изготовлении взрывчатых веществ, — например, «Бомба», «Западло с петардами», «Дымовуха на скорую руку», «Дымовая шашка»[217] и т.д.

Деструктивизм пропагандируется хакерской субкультурой[218]. Отрывок из статьи с сайта «www.xakep.ru»: «Взрывы у нас в крови. Начинается все с безобидного шифера в костре, а заканчивается терактами в Америке. Про баллоны от дихлофоса я вообще молчу»[219]. Это подтверждает, что субкультура «хакеров» вызывает интерес и у компьютерщиков, не преступивших закон, так как они нередко разделяют ее интересы.

Также респондентам было предложено определить, какая деятельность в Интернет является вредной персонально для них и общества (табл. 17).

Анализ показывает, что мнение группы «Профессионалы» сильно отличается от других отвечающих. Если они расценивают распространение информации по компьютерным преступлениям как менее вредное явление, чем другие опрашиваемые («Профессионалы» — 51,18%, «Гуманитарии» — 75,83%, «Не пользующиеся Интернет» — 75,86%), то распространение средств для совершения преступлений кажется им более опасным, чем остальным

---

[217] Доступно из электронной версии журнала по ссылкам: http://www.xakep.ru/post/14477/default.asp, http://www.xakep.ru/post/14733/default.asp, http://www.xakep.ru/post/16422/default.asp, http://www.xakep.ru/post/17568/default.asp.

[218] Более того по одной из версий именно с розыгрышами со взрывам и аморальными выходками студентов связано появление слова «hack».

[219] Западло с петрадами [Электронный ресурс] // Официальный сайт журнала «Хакер». — Режим доступа: http://www.xakep.ru/post/14477/default.asp.

(«Профессионалы» — 55,12%, «Гуманитарии» — 34,23%, «Не пользующиеся Интернет» — 37,93%). Также показательно отрицательное отношение к спаму в этой группе, что, скорее всего, вызвано необходимостью сталкиваться с этой проблемой каждый день. При этом лица, которые не пользуются Интернет, отнеслись к принудительной рассылке электронной почты очень лояльно, — всего 4,6% высказались против, так как им трудно оценить в полном объеме все негативные последствия от спама и почувствовать их на себе. Выходит, чем больше человек пользуется Интернет, тем негативней его отношение к спаму. Так как количество пользователей Интернет и количество проводимого времени в сети растет, то в будущем отношение к спаму будет еще более негативным.

Таблица 17

Вопрос: Какая деятельность в Интернет является вредной для Вас и общества?

Вид деятельности	Профессионалы	Гуманитарии	Не пользующиеся Интернет
Распространение программных средств для совершения компьютерных преступлений	55,12%	34,23%	37,93%
Принудительная рассылка электронной почты	63,78%	55,7%	4,6%
Вербовка в националистические и террористические организации	72,44%	75,84%	86,21%
Иные	3,15%	6,71%	0%

Мнение респондентов по вопросу, кто должен контролировать Интернет и должно ли государство усилить меры государственно-правового регулирования распространения определенной информации, представлено в таблицах 18 и 19.

Представляется, что «Профессионалы» больше рассчитывают на личный контроль, то есть они сами выбирают, что им смотреть, но в то же время 54,55% согласны с тем, что государственный контроль должен быть жестче. Объяснить это можно тем, что первая группа достаточно квалифицированна, чтобы самостоятельно избавиться от получения неприятной им информации, они обладают необходимыми для этого знаниями и профессиональными навыками. Большинство, например, порнографических порталов привлекает клиентов простыми техническими средствами, устанавливая на компьютер пользователя без его ведома определенные программы, которые при

следующем входе в Интернет автоматически открывают сайты нежелательного содержания[220]; чтобы защитится от таких программ, достаточно немного разбираться в Интернет-технологии.

Таблица 18

Вопрос: Какой контроль должен занимать основное место в регулировании распространения информации в Интернет? (можно выбрать несколько)

Вид контроля	Профессионалы	Гуманитарии	Не пользующиеся Интернет
Государственный	24,41%	55,03%	62,07%
Общественный	24,41%	6,71%	19,54%
Отраслевой (предоставители Интернет-услуг)	27,56%	24,16%	13,79%
Личный	63,78%	20,81%	4,6%

Группы же «Гуманитарии» и «Не пользующиеся» Интернет больше рассчитывают на государственный контроль, так как не способны самостоятельно справляться с потоком негативной информации, и в большинстве своем выступают за ужесточение государственно-правового регулирования. Представляется, что ужесточение государственного регулирования подразумевает и уголовно-правовые меры борьбы с преступностью, в том числе криминализацию некоторых общественно опасных деяний. Однако отметим, что повышение общего уровня подготовки в сфере компьютерных технологий среди пользователей, может привести к росту доли выступающих за личный контроль.

Таблица 19

Вопрос: Государственно-правовое регулирование распространения информации в Интернет должно быть жестче, мягче или таким, как есть?

Ответы	Профессионалы	Гуманитарии	Не пользующиеся Интернет
Мягче	6,3%	0%	4,6%
Таким, как есть	39,37%	20,81%	19,54%
Жестче	54,33%	79,19%	75,86%

[220] Кашапов Р.М., Наумов С.С. Проблемы с распространением детской порнографии в глобальной сети Интернет // Вестник Дальневосточного юридического института МВД России. — 2004. — № 2. — С. 74.

Анализ показывает, что большинство респондентов исследования считают государственно-правовой контроль распространения Информации в Интернет недостаточно жестким, т.е. выступают за усиление вмешательства государства в этой области, что косвенно подтверждает необходимость криминализации некоторых общественно опасных деяний.

Для выяснения мнения опрашиваемых о необходимости установления уголовной ответственности за определенные действия, были заданы два вопроса: «За распространение какой информации следует установить уголовную ответственность?»; «За какие действия, по вашему мнению, должна устанавливаться уголовная ответственность?». Мы намеренно отделили две функции Интернет: информационную как средства для распространения информации и инструментальную как средства для осуществления некоторой деятельности, отличной от распространения информации. Также в этот список включены уже криминализованные виды деяний, чтобы сравнить степень негативного отношения.

Таблица 20

Вопрос: За распространение какой информации следует установить уголовную ответственность?

Виды информации	Профессионалы	Гуманитарии	Не пользующиеся Интернет
Информация, позволяющая изготовить в домашних условиях взрывчатые вещества и взрывные устройства	48,82%	72,48%	62,07%
Информация, позволяющая изготовить в домашних условиях наркотические вещества	70,08%	75,84%	80,46%
Порнографическая продукция с участием детей	100%	89,93%	90,8%
Порнографическая продукция, доступная для просмотра детям и несовершеннолетним	70,08%	51,68%	75,86%
Информация, призывающая к расовой и межнациональной конфронтации	49,61%	58,39%	42,53%
Информация о том, как совершать компьютерные преступления и с помощью каких средств	18,11%	30,87%	19,54%

Из приведенного материала следует, что к детской порнографии негативно относятся все три группы, и хотя «изготовление и

оборот материалов или предметов с порнографическими изображениями несовершеннолетних» уже криминализовано ст. 242[1] УК РФ, но, как признают некоторые исследователи, усилия, направленные на борьбу с данным явлением, недостаточны. Например, одни из самых популярных поисковых Интернет-порталов Yandex.ru и Rambler.ru на запрос, содержащий слова «детское порно», приводят ссылки на 3 109 серверов и 21 264 страницы соответственно[221].

Если государство бездействует, то этот пробел пытается восполнить общество. Есть примеры, когда сообщество пользователей Интернет самостоятельно, правда, не всегда законно, пытается бороться с этим негативным явлением. Например, компьютерный вирус, распространяющийся по e-mail, ищет jpeg-файлы (файлы фотографий), которые могут содержать детскую порнографию. В теме послания написано: «FWD: Help us ALL to END ILLEGAL child porn NOW» (пер. на рус.: «Помогите нам всем покончить с незаконной детской порнографией»). После открытия вложенного файла вирус показывает в блокноте ряд законов, запрещающих детскую порнографию. Разослав письма с вирусом по всем адресам из адресной книги, вредоносная программа затем отсылает конфиденциальную информацию (список директорий, где червь нашел файлы фотографий, соответствующие определенному шаблону) в какое-либо из правительственных агентств[222]. Таким образом, в обществе формируется общественная инициатива за усиление противодействия распространению негативной информации в Интернет-пространстве.

Все три группы опрошенных нами лиц в большинстве своем (около 80%) выступают за криминализацию распространения информации, подробно описывающей изготовление в домашних условиях наркотических веществ. Большинство компьютерных специалистов выступает против криминализации распространения сведений о том, как совершать компьютерные преступления и с

---

[221] Кашапов Р.М., Наумов С.С. Проблемы с распространением детской порнографии в глобальной сети Интернет // Вестник Дальневосточного юридического института МВД России. — 2004. — № 2. — С. 73.

[222] Вирус на службе правительства? [Электронный ресурс]/ Cnews. Компьютерные новости. — Режим доступа: http://cnewz.ru/cgi-bin/oranews/get_news.cgi?tmpl=nl_print&news_id=118124

помощью каких средств (более 80%). Заметим, что значение данной информации не однозначно. Например, информация о способах незаконного доступа с подробным описанием содержится на сайтах для специалистов по безопасности Интернет-систем.

Результаты опроса: «За какие действия, по вашему мнению, должна устанавливаться уголовная ответственность?», представлены в таблице 21.

Таблица 21

Вопрос: За какие действия, по вашему мнению, должна устанавливаться уголовная ответственность?

Виды действий	Профессионалы	Гуманитарии	Не пользующиеся Интернет
Распространение программных средств для совершения компьютерных преступлений	29,92%	27,52%	37,93%
Принудительная рассылка электронной почты (спам)	39,37%	24,16%	4,6%
Вербовка в националистические и террористические организации	75,59%	75,84%	80,46%

Наиболее негативно все три группы опрошенных относятся к вербовке в националистические и террористические организации. Интересно, что в Интернет уже есть примеры, когда это недовольство переросло в реальные действия. Так, например, сайт «cyber underground community VS terrorism» (пер. на рус. «Общество киберандеграунда против терроризма») создан с целью борьбы с террористическими порталами[223]. На нем собираются компьютерные профессионалы и пытаются незаконными (хакерскими) методами нарушить работу протеррористических порталов.

Интересно мнение по поводу установления уголовной ответственности за спам. Наибольшее количество респондентов в группе «Профессионалы», чем в других группах, выступают за криминализацию спама, что вполне логично. Так, более развитые в технологичном плане страны (США, страны ЕС, Австралия[224]) уже при-

[223] Cyber underground community VS terrorism. http://www.peace4peace.com/

[224] SPAM ACT 2003 [Электронный ресурс]/ The Attorney General's department. — Режим доступа: http://scaleplus.law.gov.au/html/pasteact/3/3628/top.htm

няли антиспамерские законы. Есть случаи привлечения к ответственности. Например, в апреле 2005 г. австралийскими властями была обнаружена так называемая фабрика спама в городе Перт, где властями были изъяты жесткие диски и прочие улики против спамеров[225]. То есть количество граждан, недовольных спамом и поддерживающих установление уголовной ответственности, зависит от интернетизации общества, так как чем больше человек страдает от спама, тем больше недовольных. С ростом профессионализма пользователей Интернет и их количества, число лиц, негативно настроенных по отношению к спаму, увеличится. По мнению специалистов, распространение средств для совершения преступлений (29,92%) более опасно, чем распространение информации о том, как совершать компьютерные преступления (18,11%).

Представляет также интерес мнение опрошенных по поводу личности «хакера» (табл. 22).

Таблица 22

Вопрос: Кто такой, по вашему мнению, «хакер»?

Ответы	Профессионалы	Гуманитарии	Не пользующиеся Интернет
Опасный преступник	9,45%	38,25%	9,2%
Борец за свободу Интернет	0%	3,36%	13,79%
Искусный программист	90,55%	51,68%	75,86
Иное	0%	6,71%	0%

Участники опроса из группы «Профессионалы» чаще всего склонны считать «Хакера» искусным программистом (90,55%). Это, по нашему мнению, возможно по двум причинам. Во-первых, благосклонное отношение к компьютерной преступности; во-вторых, термин «Хакер» действительно в среде компьютерных профессионалов очень часто используется по отношению к искусным программистам. Группа «Гуманитарии», в большинстве своем, также считает хакера искусным программистом (51,68%), но все же значительное число опрошенных из этой группы (38,25%) относят «хакера» к опасным преступникам. В группе «Не пользующиеся Интернет» большинство тоже считает «хакера»

[225] Properties raided by authorities searching for spam factory [Электронный ресурс] / Sophos reports. Sophos. Arcticles. — Режим доступа: http://www.sophos.com/pressoffice/news/articles/2005/04/sa_spamfactory.html

искусным программистом (75,86%), но что характерно, данной группе свойственно идеализировать образ хакера и считать его борцом за свободу Интернет (13,79%). По нашему мнению, это вызвано недостатком знаний в данной области и растиражированным через художественные произведения героическим образом «хакера»[226]. Приукрашивать образ хакеров свойственно и некоторым ученым, — например, Ю.М. Батурин называет хакеров «электронными корсарами»[227].

Результаты проведенного нами исследования позволяют сделать ряд обобщающих выводов. В частности, что отношение компьютерных профессионалов к Интернет-преступности и к вопросу о регулировании сети действительно отличается от мнения людей, не являющихся профессионалами в компьютерных технологиях и не пользующихся Интернет. «Компьютерщики» не считают опасным деяниям распространение информации о взломах, зато считают опасным распространение программных средств для совершения преступления.

Все три группы лиц достаточно негативно относятся к распространению детской порнографии и распространению информации о том, как изготовить наркотики в домашних условиях. Опасность подрыва нравственных устоев от распространения порнографии среди несовершеннолетних очевидна, и поэтому более 50% опрошенных в трех группах высказалось негативно против такого рода деятельности. В случае же с терроризмом общественная опасность возрастает многократно и около 80% респондентов во всех группах высказывается за установление уголовной ответственности за вербовку в националистические и террористические организации в Интернет через специально созданные сайты или каким-либо другим образом.

«Гуманитарии» и «Не использующие Интернет» последовательно выступают за введение государственно-правового контроля и за ужесточение мер юридической ответственности. «Профессионалы» хотя и разделяют усиление государственного контроля, но все-таки считают, что основной контроль должен быть личным.

---

[226] Фильмы: «Хакеры», «Военные игры», «Взломщик». Книга С. Лукьяненко «Лабиринт отражений» и т.д.

[227] Батурин Ю.М., Жодзишкий А.М. Компьютерная преступность и компьютерная безопасность. — М.: Изд-во Юрид. лит., 1991. — С. 12.

У всех трех групп различается отношение к «хакеру», «Профессионалы» его относят к искусным программистам. Некоторые из группы «Не использующие Интернет» даже идеализируют хакера, называя его борцом за свободу Интернет.

Вызывает опасение то, что общество само пытается восполнить пробелы в правовом (в т.ч. уголовно-правовом) контроле Интернет, иногда незаконными методами. В истории России достаточно примеров. Если право по каким-либо основаниям не исполняет роль регулирования и охраны общественных отношений, то эти функции берут на себя отдельные лица или группы людей. Например, в начале 90-х, когда законодательство запаздывало, были известны примеры того, что проблемы решались вне правового поля («по понятиям»).

В наши дни общество само пытается бороться с распространением общественно опасной информации, размещенной в Интернет, в том числе и незаконными способами. В этой связи можно прогнозировать, что в связи с отставанием в области государственно-правового регулирования и ростом профессионализма пользователей российского Интернет, количество данных случаев будет расти. Поэтому необходимы дальнейшие более глубокие криминологические и уголовно-правовые исследования в этой области в целях разработки адекватных мер противодействия Интернет-преступности с учетом мнения российского общества.

3.2. Понятие и формирование субкультуры «хакеров»

Интернет в настоящее время является не только принципиально новым средством массовой коммуникации, он охватывает практически все сферы человеческой деятельности. Многие процессы успешно переносятся из физического мира в виртуальный «искусственный» мир сети. Глобальная сеть создает условия для формирования виртуальных общностей, генерирует языковые формы нового типа, стирает границы между государствами, игнорирует расстояния, разъединяющие людей, и в конечном счете порождает специфические формы культуры.

Некоторые исследователи выделяют общность пользователей Интернет как своеобразную субкультуру, одной из основ которой

является информационный либерализм[228]. В Хакеров можно назвать «радикальным крылом» данной субкультуры, так как ради свободы доступа к информации они готовы к совершению ряда преступлений.

Согласно современной точке зрения, субкультура — это «особая сфера культуры, целостное суверенное образование внутри господствующей культуры, отличающееся собственным ценностным строем, обычаями, нормами»[229].

Н.Л. Денисов считает, что субкультура — это совокупность норм и правил поведения, традиций, обычаев и внешней атрибутики, которые существуют внутри определенной социальной микрогруппы лиц, объединенных каким-то общим интересом (профессиональным или иным); поддерживаются всеми членами этой группы и отличаются от общепринятых в обществе. Она обычно определяется как система совместных верований, отношений и символов, дифференцирующих определенную микрогруппу в пределах большого культурного сообщества[230].

Разделяя мнение, что субкультура понятие относительное и рассматривать ее можно только как особую культуру внутри некоторой более распространенной, предполагается, что для удобства следует разделить субкультуру на духовную и материальную составляющие. К духовной части относятся основные идеологические предпосылки и моральные нормы, нравственные ценности. К материальным — все внешние проявления субкультуры. Например, обычаи, ритуалы, стиль в одежде. И духовно-материальные проявления — это произведения искусства, которые несут в себе как материальную, так и духовную сторону, — например, кинофильмы.

Представляется, что такой подход позволяет объединить и выделить общее у всех компьютерных и Интернет-преступников,

---

[228] Смирнова И.А. Виртуальное пространство культуры [Электронный ресурс]: Материалы научной конференции 11—13 апреля 2000 г. — СПб.: Санкт-Петербургское философское общество, 2000. — С.148—149. — Режим доступа: http://anthropology.ru/ru/texts/smirnova_ia/virtual_53.html

[229] Гуревич П.С. Субкультура // Культурология. XX век: Энциклопедия. Т. 2. — СПб., 1998. — С. 236.

[230] Денисов Н.Л. Влияние криминальной субкультуры на становление личности несовершеннолетнего преступника: дис. ... канд. юрид. наук: 12.00.08. — М., 2002. — С. 19.

несмотря на явные различия в социальных позициях, ролях, видах деятельности, потребностно-мотивационной сфере и в ценностно-нормативных характеристиках. Хотя духовная часть субкультуры в некоторой мере охватывается понятием культура личности, ее материальная и духовно-материальная составляющие остаются за рамками такого казалось бы емкого и универсального понятия, как личность преступника. Переход к категории субкультур позволяет нам проследить направления развития идеологии и духовно-нравственной сферы хакеров, выявить общие моменты и проследить связи с остальным криминальным миром, отследить механизмы воспроизводства и распространения Интернет-преступности.

Отметим, что, рассматривая личность компьютерного, кибер- или Интернет-преступника, исследователи так или иначе затрагивали термины хакер, крэкер, пытаясь, таким образом, их классифицировать и более того, найти таким классификациям применение на практике. Наиболее часто встречающаяся, кочующая из диссертации в диссертацию и из книги в книгу классификация: Белые воротнички, Шутники, Вандалы, Взломщики-профессионалы, Кибергангстеры, Компьютерные шпионы и т.д в разных вариациях[231]. Несмотря на популярность, отметим убогость данной классификации и отсутствие хоть каких-либо критериев данной классификации. Например, Шутники — наименее опасная часть кракеров, основная цель которых известность, достигаемая путем взлома компьютерных систем и внесением туда различных эффектов, выражающих их своеобразное чувство юмора[232]. Есть, конечно, удачные попытки типологии и классификации, которые имеют глубокую обоснованность и полезны как в теоретическом плане, так и на практике[233].

---

[231] См.: Гаджиев М.С. Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан): дис. ... канд. юрид. наук: 12.00.08. — Махачкала, 2004. С. 70—71.; Ушаков С.И. Преступления в сфере обращения компьютерной информации (теория, законодательство, практика): дис. ... канд. юрид. наук: 12.00.08. — Ростов-на-дону, 2000. — С. 142—144. и т.д.

[232] Старичков М. В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики: дис. ... канд. юрид. наук: 12.00.08. — Иркутск, 2006. — С. 141—143.

[233] Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение: дис. ... канд. юрид. наук: 12.00.08. — М., 2003; Геллер А.В. Уголовно-правовые и криминологические аспекты обеспечения защиты электронной информации и Интернета: дис. ... канд. юрид. наук: 12.00.08. — М., 2006.

Представляется, что, несмотря на всю ценность этих исследований, они не могут дать ответов на важные вопросы, связанные с личностью компьютерного и Интернет-преступника. Например, хакеры — это новая специализация традиционного преступного мира или это новая социальная формация, которая со временем обрела преступные формы? Как происходит воспроизводство компьютерной и Интернет-преступности? Почему в странах, где социально-экономические предпосылки для существования Интернет-преступности не так сильны, ее распространенность высока? и т.д.

Действительно ли социокультурное образование хакеров является субкультурой? По крайней мере, должен присутствовать набор характерных черт, которые позволяют говорить о хакерах как о субкультуре. Это следующие черты: специфический стиль жизни и поведения; свойственные данной социальной группе своеобразные нормы, ценности, мировосприятие; наличие более или менее явного инициативного центра, генерирующего идеи[234].

Первые хакеры появились в начале 60-х в Массачусетском технологическом институте, который считается одним из лучших технологических вузов США. Слово «hack» имеет множество значений, в том числе «разрубать, кромсать, разбивать на куски». Наиболее часто возникновение этого термина приписывают лаборатории «моделей перемещения железнодорожных составов» (Tech Model Railroad Club) при Массачусетском технологическом институте (в этом институте работало большинство разработчиков основ прообраза сети Интернет). Он означал «разбор до винтика» электрических поездов, путей и стрелок, для поиска нового способа ускорить движение поездов. Позже, с появлением компьютеров, этот термин был перенесен на «оригинальный ход в программировании или использовании программного обеспечения, в результате которого компьютер позволял осуществлять операции, ранее не предусмотренные или считавшиеся невозможными»[325]. В то время это было занятие для гениальных компьютерных спе-

---

[234] Левикова С.И. Молодежная субкультура. — М., 2004. — С. 12.

[235] Михаил Вершинин. Современные молодежные субкультуры: хакеры [Электронный ресурс] / Сайт практической психологии ПСИ-ФАКТОР — Режим доступа: http://www.psyfactor.org/lib/vershinin4.htm

циалистов, которое занимало их пытливый ум и не приносило никакой материальной выгоды[236].

В 70-х годах развитие автоматических и цифровых телефонных сетей привело к появлению первой специализации в субкультуре «фрикеров». В это время хакерам свойственна некая элитарность, субкультура похожа на закрытое общество. Секреты технологии взлома тогда можно было узнать только от определенного круга людей, и при этом надо было самому обладать достаточной квалификацией, либо разбираться в машинном коде с помощью простого анализа машинных инструкций, если речь идет о программном обеспечении, либо разобрать винтик за винтиком, если речь идет об аппаратном обеспечении[237]. Такая закрытость и не распространенность была связана со сложностью и недоступностью компьютерных систем в то время.

Впоследствии субкультура начала открыто распространять свои ценности посредством кино, музыки, журналов. Фильм о хакерах «Военные игры» имел огромный успех. Сюжет повествует о хакере, взломавшем компьютерную сеть северо-американской системы противоракетной обороны и чуть было не развязавшем третью мировую войну. Этот фильм пока еще не провозглашает каких-либо идеологических посылов, но привлекает внимание к огромным возможностям, предоставляемым компьютерами и компьютерными сетями. В этом фильме уже можно проследить некоторый подростковый компьютерный нигилизм. Так, например, главный герой заявляет о том, что не считает звонки за чужой счет преступлением[238].

С 1984 г. начинает регулярно издаваться ежемесячник «2600». Его редактировал Эрик Корли, который взял хакерский псевдоним Эммануил Голдштейн у главного героя культового романа-антиутопии «1984» Джорджа Оруэлла. Через год после этого стал выходить он-

---

[236] Крис Касперский. «Философия хакерских атак» [Электронный ресурс] // Репорт.ру. — Режим доступа: http://hacker.report.ru/material.asp?MID=388

[237] Это достаточно нетривиальная задача, даже для специалиста, прим. автора.

[238] V. DeMarco, It's not just fun and «War Games» - Juveniles and Computer Crime [Электронный ресурс]/ Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice. — Режим доступа: http://www.cybercrime.gov/usamay2001_7.htm

лайновый журнал «Phrack». Оба издания публиковали обзоры и советы для хакеров[239]. Эммануил Голдштейн в 1995 г. стал прообразом героя известного кинофильма «Хакеры», где компьютерные преступники представлены как сформировавшаяся субкультура. Во-первых, провозглашаются ценности хакеров, имеющие серьезное философское обоснование; во-вторых, преподносится целостный образ хакера, который отличается стилем жизни, одеждой и общением. В-третьих, в этом фильме преступное компьютерное сообщество противопоставляется государству, при этом хакеры представлены в более благоприятном свете, чем сотрудники федеральных служб.

В настоящее время субкультуру хакеров можно считать сформировавшейся. Они имеют специфический стиль жизни; свойственные данной социальной группе своеобразные нормы, ценности, предпочтительные модели поведения и внешние отличительные атрибуты.

В основе идейной базы хакеров лежит либерализация доступа к информации. «Мы исследуем, и вы называете нас преступниками. Мы в поисках знаний и вы называете нас преступниками» — это отрывок из известного манифеста хакеров (The Hacker Manifesto), написанного хакером под псевдонимом Mentor[240]. Этот тезис поддерживается большинством сетевого сообщества. Так, например, даже в Китае, где традиции либерализма не так распространены, как в Америке, можно наблюдать тенденцию к борьбе «жителей сети» (netizens) за свободное освещение важных событий посредством Интернет[241].

При этом авторы в поддержке свободы информации не голословны, зачастую их лозунги подкрепляются серьезными и продуманными аргументами, культурно, философски, логически обоснованными. Например, К. Касперский: «Ситуация дошла до логического

---

[239] Крис Касперский. «Философия хакерских атак» [Электронный ресурс] // Репорт.ру. — Режим доступа:http://hacker.report.ru/material.asp?MID=388

[240] Mentor. Hacker Manifesto, Written on January 8, 1986. http://project.cyberpunk.ru/idb/hacker_manifesto.html

Другой отрывок из этого манифеста произносится в фильме Хакеры, который упоминался выше См. также: Chirillo J. Hack Attacks Revealed. — New York: Wiley Computer Publishing, 2001. — P. 83—87.

[241] Xiao Qiang. Cniha's Virtual Revolution [Электронный ресурс] // Project Syndicate. — Режим доступа: http://www.project-syndicate.org/commentaries/commentary_text.php4?

абсурда, и в воздухе запахло бунтом. Бунтом против тоталитаризма демократического режима, когда один пронырливый коммерсант отнимает у человечества то, что принадлежит ему по праву. Информация — общедоступный ресурс, такой же, как вода и воздух. Мы дети своей культуры. Наши мысли и суждения, которые мы искренне считаем своими, на самом деле уже давно представляют собой комбинацию уже давно придуманного и высказанного. Удачные находки, яркие идеи — все это результат осмысления или переосмысления. Когда-то услышанного или прочитанного»[242]. Представляется, что для хакера право на свободу информации является более очевидным и логичным, чем патентные, авторские права, право государственной тайны. То есть в рамках субкультуры хакеров право на информацию просто не действует в силу того, что «для функционирования в рамках определенной культуры право обязано быть признано и оправданно в качестве такового»[243], и что «право должно быть совместимо с нравственными ценностями человека»[244].

Можно выделить также и неприятие ими потребительской культуры. Об этом свидетельствует отрывок из «Библии хакера» (cracking notes), написанной хакером под псевдонимом «Orc + », который пронизан ненавистью к существующему общественному устройству[245]. Призыв борьбы с обществом потребления пере-

---

[242] Касперски К. Техника отладки программ без исходных текстов / К. Касперски. — СПб.: БХВ-Петербург, 2005. — С. 4.

[243] Данильян О.Г. Философия права: Учебник / О.Г Данильян, Л.Д. Байрачная, С.И. Максимов и др.; Под. ред. О.Г. Данильяна. — М.: Изд-во Эксмо, 2006. — С. 288.

[244] Нерсесянц В.С. Философия права: Учебник для вузов. — М.: Изд-во НОРМА, 2004. — С. 621; Рябцев Р.А. Современная правовая реформа в России и правосознание: дис. ... канд. юрид. наук: 12.00.01. — Ростов-на-дону, 2005. — С. 53., Кочетков А. Меры противодействия криминальной идеологии в культуре // Законность. — 2002. — № 4. — С. 51—52.

[245] «Почему люди не смотрят на звезды, не любят друг друга, не чувствуют ветра, не запрещают вонять машинам там, где живут и едят... при этом ставя себя на «передовой край технологии»? Почему они больше не читают поэмы? Нет больше поэзии, в этой серой толпе рабов поэзия скоро будет запрещена, вы не можете ПОТРЕБЛЯТЬ, как вы бы этого хотели, в этом фарсе общества вы связаны потреблением, это единственное, чего они от вас хотят... парни, временами я чувствую себя удачно размещенной нейтронной бомбой, которая однажды убьет всех бесполезных зомби и покинет благородные книги и не откупоренную хорошую водку.»

кликается с идеологией других молодежных субкультур, что придает данной субкультуре еще большую популярность. Так, во многих текстах песен рок-групп присутствуют подобные строчки, а рок-музыка популярна среди молодежи.

Мотив отрицания культуры потребления и противопоставления существующему обществу присутствует и во многих других молодежных субкультурах, таких как хиппи, панки, рокеры и т.д.; все они поддерживают так называемый анти-консьюмеризм, движение против культуры потребления (консьюмеризма — англ. consumerism), направленное на более скромное, избирательное потребление благ с учетом экологических принципов и естественных духовных потребностей человека, освобождение от рекламного «зомбирования» и т. п[246]. Такой призыв поддерживают и антиглобалисты. Субкультура хакеров очень схожа со многими молодежными культурами своей идеологией, ее следует скорее относить к молодежным субкультурам, чем к криминальным.

Важный аспект идеологии — это вера в способность компьютера изменить жизнь к лучшему; неприятие каких-либо авторитетов и отрицание расовых, религиозных, социальных различий. Вся жизнь хакера: работа и досуг, музыка, книги и фильмы — так или иначе связаны с компьютером. Они надеются, что благодаря информационным технологиям и особенно Интернет возможно достижение истинного равенства и равноправия, когда не будет важен социальный статус и цвет кожи, что подтверждают слова Mentor-a: «Это наш мир сейчас ... Мир электронов, маршрутизаторов, красоты двоичного кода» ... «Мы существуем без цвета кожи, национальности и религиозных предубеждений»[247]. В свою очередь, неприятие авторитетов характерная черта практически всех молодежных субкультур.

Субкультура хакеров существенно отличается от других криминальных культур, но в то же время можно найти и некоторые сходства. Так, например, В.В. Тулегенов выделяет несколько отли-

---

[246] Anti-consumerism [Электронный ресурс] // Толковый англо-русский словарь «Экономика, социология, политология». — Режим доступа: http://ecsocman.edu.ru/db/dict/4693/dict.html?wd=6924

[247] «This is our world now... the world of the electron and the switch, the beauty f the baud.» ... «We exist without skin color, without nationality, without religious bias... and you call us criminals.»

См: http://project.cyberpunk.ru/idb/hacker_manifesto.html

чий криминальных субкультур. Они отличаются быстрой изменчивостью, так как преступный мир всегда отличался высокой адаптивностью и умением приспосабливаться к изменяющимся условиям[248]. Это относится и к хакерской культуре. В остальном субкультура Интернет-преступников сильно отличается от криминальной субкультуры.

Во-первых, В.В. Тулегенов утверждает, что криминальные субкультуры не оставляют материального наследия, то есть не располагают какими-либо материальными носителями, кроме самих преступников, и передаются из уст в уста. В случае с хакерами это не так. Существует целый хакерский эпос. История известных хакеров растиражирована через СМИ, Интернет, книги и кинофильмы. У хакеров есть своя «библия», а многочисленные Интернет-порталы рассказывают, как стать хакером, как одеваются хакеры и как они думают. Хотя у криминальной субкультуры есть свой жаргон, клички, кодекс, идеология, и они не так доступны, как элементы субкультуры хакеров[249].

Во-вторых, криминальная субкультура — это закрытая система, она обладает своими скрытыми, чаще всего опасными установками, противоречащими общественным. Субкультура хакеров тоже закрытая система, но при этом хакерские ценности имеют хорошо проработанную философскую основу, и это придает некую легитимность хакерским идеям. Так, например, согласно проведенному нами исследованию 14,29% людей, вообще не пользующихся Интернет, считают хакера «борцом за свободу Интернет». Термин «хакер» используют не только для того, чтобы показать преступную наклонность личности, но и подчеркнуть его исключительные способности в сфере компьютерных технологий. По нашим исследованиям, более 90% специалистов в сфере информационных технологий и более 50% пользователей Интернет без компьютерного образования считают хакера прежде всего «искусным программистом».

---

[248] Тулегенов В.В. Криминальная субкультура и ее криминологическое значение: дис. ... канд. юрид. наук: 12.00.08. — Ростов-на-Дону, 2003. — С. 17.

[249] Исключением правда является криминальный фольклор. См.: Дубягина О.П. Криминологическая характеристика норм обычаев и средств коммуникации криминальной среды: автореферат на соискание степени ... канд. юрид. наук: 12.00.08. — М., 2008. — С. 20.

Вот еще один отрывок из «Библии хакера»: «В это трудно поверить при сегодняшней демократии и более... даже если я и сделаю... все бесполезные зомби скорчат несчастное лицо типичного идиота, в чем действительно будут похожи на самих себя и не позаботятся ни о чем больше, как о добывании баксов и защите своих же партнеров. Рабы выбирают людей, которых видят по телику, как если бы египтяне голосовали бы за их фараонов, подбадриваемые плетками надсмотрщиков...»[250].

В этих строках можно увидеть провозглашаемое хакерами их возвышение над обществом, при этом в философии хакеров используются не новые и уже набравшие популярность идеи. Хакеры гордо провозглашают себя не преступниками, а борцами против рабства.

В обрядах и поведении хакеров и представителей других криминальных субкультур можно найти сходство. Самое первое, что бросается в глаза, — это использование псевдонимов, во многих субкультурах используются клички, псевдоимена, прозвища. В хакерской среде их называют «никами» (англ. nick, nickname — прозвище, кличка, уменьшительное имя, псевдоним). Псевдоимена приняты не только в преступной Интернет-субкультуре, но и во всем Интернет-сообществе. В отличие от псевдоимен в криминальной среде — «кличек», «ник» каждый выбирает себе сам.

Как и в других криминальных субкультурах, в «никах» могут быть отражены: характерологические особенности и особенности поведения; трансформированные фамилии и имена; статус в группе; особенности внешности или социального статуса; предпочтения в музыке, литературе, искусстве; специфика преступной деятельности и места совершения.

Проанализировав 112 Интернет-сайтов, на которых размещены материалы для хакеров, мы установили, что «ник» хакеры пишут преимущественно латинским алфавитом; из 1000 выявленных

---

[250] Созвучно с таким высказыванием: «Мне думается, сама искусность, с какой XIX век обустроил определенные сферы жизни, побуждает облагодетельствованную массу считать их устройство не искусным, а естественным. Этим объясняется и определяется то абсурдное состояние духа, в котором пребывает масса: больше всего ее заботит собственное благополучие и меньше всего - истоки этого благополучия», Ортега-и-Гассет Х. Восстание масс. — М.: АСТ: Ермак, 2005. — С. 52—53.

нами «ников»[251] только четыре были написаны русским алфавитом. На наш взгляд, это объясняется несколькими причинами. Во-первых, русский алфавит поддерживается не во всех компьютерных системах, во-вторых, в языках программирования и системных файлах самых распространенных операционных сред компьютера (Windows, UNIX и т.д.) чаще используют латинский алфавит. Обращает внимание различие с «никами» людей, не разбирающихся в компьютерах. Хакеры не используют связку ник-число в своих псевдоименах (например, dimon1976, xaker3 и т. д.). Специалисты объясняют это тем, что такие имена свидетельствуют о некомпетентности человека его использующего, так как автоматически предлагаются при регистрации на Интернет-порталах как альтернатива в случае, если имя, которое хочет использовать человек, занято другим (например, если занято имя dimon — сайтом автоматически предлагается dimon2 или dimon1976).

По нашим исследованиям, в 21,6% случаев «ник» был взят из книг, кинофильмов и компьютерных игр; 7,1% псевдоимен — компьютерные термины. Всего 4,3% — это собственные имена. Некоторые хакерские группы используют имена для обозначения принадлежности друг другу. Например, они берут в качестве «ников» имена героев из какого-нибудь рассказа, пытаясь соблюсти совпадение иерархии и черт героев рассказа с отношениями в группе и характерами ее членов. Также для обозначения принадлежности к какой-либо группе может использоваться префикс в слове, либо так называемое «обозначение клана» — название группы, записанное в квадратные скобки (например, neo[Matrix] — хакер «neo» из клана матрица), которое пишется как в начале «ника», так и после. Данное обозначение часто используется и «геймерами»[252] для идентификации игроков из одной команды.

Согласно нашему исследованию, в хакерской среде не встречаются клички, аналогичные тюремным или общекриминальным, а также унижающие достоинство или высмеивающие недостатки. Во-первых, каждый придумывает себе псевдоним сам, а во-вторых, скорее всего преступная субкультура хакеров пока мало пересекается с общекриминальной.

---

[251] Мы брали подряд все уникальные «ники», встречающиеся в комментариях к статьям и в записях форумов.

[252] Геймер — от англ. gamer — игрок, в России используется по отношению к фанатам компьютерных игр.

Как и во всех субкультурах, у преступной субкультуры хакеров существует свой жаргон. В отличие от общекриминального «воровского» жаргона, который является производным от русского языка, современный язык хакеров в России наполнен иностранными словами. Например, «баг» (от англ. bug — жучок, ошибка в программировании)[253] означает уязвимость в программах, которую можно использовать для совершения преступления. Хакерский язык недоступен обычным пользователям, хотя многие слова используются и в непреступной среде компьютерных профессионалов.

Знание хакерского сленга обязательно для чтения информации на сайтах Интернет-преступников. Большинство сообщений изобилует терминами, которые отсутствуют в обычном толковом словаре русского языка, что автоматически отсекает ненужных, не смыслящих в компьютерных технологиях читателей[254].

Так как порталы, рассказывающие о методах совершения Интернет- преступлений, привлекают не только хакеров, но и специалистов по компьютерной безопасности, а иногда личностей, которые успешно совмещают то и другое[255], сленг российских Интернет-преступников скорее близок к языку законопослушных компьютерных профессионалов, чем к «воровскому». Исследовав популярные сайты, ориентированные на компьютерных преступников, мы не нашли ни одного применения слов воровского жаргона. Вышесказанное свидетельствует о том, что хотя *общекриминальная субкультура и культура хакеров имеют некоторое сходство, но все-таки достаточно далеки друг от друга.*

С данным фактом согласны и некоторые идеологи хакерского движения. Так, К. Касперски, автор книг «Техника и философия хакерских атак», «Техника отладки программ без исходного кода» и т.д., описывает хакера следующим образом: «Бытует мнение о существовании некоторых признаков принадлежности к хакерам.

---

[253] Баг в ИЕ (отображение html в изображениях). Как юзать [Электронный ресурс] // портал «antichat.ru». — Режим доступа: http://forum.antichat.ru/thread9910.html

[254] Некоторые слова имеют совершенно другое значение в русском языке, например, «инъекция» — это одна из разновидностей методов взлома компьютера.

[255] Сергей Шевченко. Профессия — хакер (часть II) [Электронный ресурс] / Центр исследования компьютерной преступности. — Режим доступа: http://www.crime-research.ru/analytics/hacker12/

Это длинные (нечесаные) волосы, пиво, сигареты, пицца в неограниченных количествах и блуждающий в пространстве взгляд... подобные признаки являются не причиной, а следствием. Привязанность к компьютеру заставляет экономичней относится к свободному времени, порой питаясь урывками и на ходу...Длинные волосы? Да, они свойственны всем компьютерщикам (и не только им), а вовсе не исключительно хакерам, как, кстати, и все другие хакерские признаки». Представляется, что хакеров и компьютерную (непреступную) субкультуру объединяет общий предмет обожания — «компьютерные технологии», в том числе Интернет.

Если говорить об остальных внешних атрибутах хакерской культуры, то необходимо упомянуть, что в отличие от других преступных субкультур, хакеры имеют собственные периодические издания, художественную литературу, кинофильмы, видеоролики, постеры. Другие категории преступников довольствуются только специализированными Интернет-сайтами; существуют Интернет-порталы, ориентированные, например, на наркопреступника.

Трудно представить ситуацию, что в России регулярно выходил бы журнал «Карманник» и где были бы рекомендации, как избежать уголовной ответственности, как эффективней совершать преступления и в приложении к журналу находился бы набор лезвий для разрезания кошельков. А вот журнал «Хакер» выходит в России с 1999 г. В ноябрьском номере за 2005 г. можно встретить статьи о том, как украсть персональную информацию из популярной программы обмена сообщениями ICQ (сокр. — от «I seek you» — Я ищу тебя); как незаметно проследить за чужим компьютером, чтобы узнать, какие сайты с него посещают, как получить незаконный доступ к ядру системы форума[256]; как внедрить вредоносную программу в ELF файлы (формат файла) и т.д. Кроме того, журнал продается с приложением: двумя CD-дисками, на которых есть видео осуществленных взломов, программы для взлома и масса уже взломанных лицензионных программ (пиратские копии лицензионных программ нельзя использовать без взлома, так как они содержат защиту от нелегального использования)[257].

---

[256] Форум — сайт для обсуждения различных тем. Кто-нибудь формирует проблему и другие посетители форума ее обсуждают.

[257] Само распространение таких программ уголовно наказуемо, например, распространение некоторых программ для взлома квалифицируется по ст. 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ».

В настоящее время одним из самых распространенных видов вредоносных программ являются программы, предназначенные для сбора информации и программы для несанкционированного доступа к ЭВМ либо другим программам[258]. Именно такие программы и распространяются на диске с журналом. Например, THC PPTP bruter 0.1.4 (THC - имя хакерской команды, bruter — насильник, жестокий человек) — взломщик паролей и kismet-2005-08-R1 (kismet — рус. судьба, рок) — программа для перехвата и расшифровки информации, передаваемой по сети, и т.д.

Кроме периодических изданий, у хакеров есть и художественные фильмы, в которых описывается образ их жизни и пропагандируются их жизненные ценности. Иногда за основу сюжета берутся реальные события, — так, например, фильм «Взлом» (англ. «Takedown», 2000 г.) рассказывает о жизни известного во всем мире хакера Кевина Митника. В нем не только освящены технические подробности взломов (фильм наполнен компьютерной терминологией), но и заявлено о неспособности спецслужб справиться с такого рода «гениями». По ходу фильма ФБР долгое время не может поймать компьютерного преступника, и лишь при помощи независимого специалиста по безопасности компьютерных систем случайно ловит его. С материалами данного уголовного дела можно ознакомиться на сайте департамента юстиций США, где Митник назван «прославленным» (англ. «notorious») хакером[259].

Значения литературы и кино для хакеров не стоит недооценивать. Для профессиональных хакеров большинство сюжетов кажутся смешными и далекими от реальности, но для основной массы (особенно для подростка) хакерские произведения искусства формируют идеал, к которому надо стремиться, в легкой и доступной форме прививают ценности хакера, демонстрируют модели поведения. При этом образ хакера сильно романтизирован и поэтому привлекателен.

---

[258] Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. В. М. Лебедев. — 5-е изд., доп. И испр. — М.: Юрайт-Издат, 2006. — С. 693.

[259] Kevin Mitnick to nearly four years in Prison [Электронный ресурс]/ Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice. — Режим доступа: http://www.cybercrime.gov/mitnick.htm

Чтобы понять, как много выпускается книг для хакеров, достаточно ввести в любой популярной поисковой системе (Yandex.ru, Rambler.ru, Google.ru и др.) запрос «книги для хакера», здесь можно найти книги с названиями «Супер-хакер», «Как стать хакером», «Секреты хакеров» и т.д.

Представляется, что главным выводом из вышесказанного является доказанное существование субкультуры хакеров и ее широкая распространенность в настоящее время. Данная субкультура в российском Интернет заимствована на западе и пока имеет мало общего с субкультурой криминального мира.

В связи с изложенным предлагается следующее определение преступной субкультуры хакеров: это совокупность идей, ценностей, обычаев, традиций, норм поведения, направленная на организацию образа жизни, целью которого является совершение компьютерных преступлений, их сокрытие и уклонение от ответственности. Ценностный комплекс данной субкультуры служит для легитимации и популяризации идеи хакерства в обществе.

Представляется, что одним из важных вопросов является, как соотносятся друг с другом субкультура «хакеров» и преступная субкультура в Интернет. Либо это тождественные понятия, либо преступная субкультура включает в себя субкультуру хакеров, либо данные явления существуют отдельно.

Некоторые ученые считают, что «хакерская» субкультура — это субкультура всех компьютерщиков — и преступных, и законопослушных. Например, П. Ломакин и Д. Шрейн утверждают, что в настоящее время термин «хакер» употребляется в двух значениях: с одной стороны, это человек, который прекрасно знает компьютер и пишет хорошие программы, а с другой — незаконно проникающий в чужие компьютерные системы с целью незаконного получения информации[260].

А некоторые исследователи считают, что субкультура хакеров выходит далеко за рамки компьютерных технологий. М. Левин говорит о том, что хакерский взгляд на мир не ограничивается лишь культурой хакеров-программистов, хакерский подход применяется и в таких областях, как электроника или музыка[261].

---

[260] Ломакин П., Шрейн Д. Антихакинг. — М.: Майор, 2002. — С. 7.

[261] Левин М. Как стать хакером: Интеллектуальное руководство по хакингу и фрикингу / Максим Левин. — 3-е изд. — М.: ЗАО «Новый издательский дом», 2005. — С. 6.

Многие исследователи сходятся на том, что хакер отличается особым хакерским подходом, а не тем, что совершает Интернет-преступления[262]. К. Касперски утверждает, что первые хакеры появились задолго до появления компьютеров, и что главная черта хакеров — это нетривиальное решение задач, за гранью восприятия мира. Им мало видеть предмет в трех измерениях. Для хакеров каждый предмет — это, прежде всего, объект со своими свойствами, методами и причинно-следственными связями[263]. Несмотря на это, заметим, что в настоящее время субкультура хакеров и субкультура преступников в Интернет очень близки и часто употребляются как синонимы. Сами Интернет-преступники называют хакингом (англ. — «hacking») именно взлом, а не поиск уязвимостей или какую-либо другую деятельность. Хотя термины «хакер», «хакинг» употребляются не по назначению, но, например, «бандит» также можно услышать в обычной речи по отношению к перешалившему ребенку; то есть хакер, прежде всего, преступник. Наиболее удачно по этому поводу выразился М.М. Менжега, который заметил, что в литературе, связанной с компьютерами (включая юридическую), слово «хакер» трактуется совсем по-разному, причем толкование ограничивается лишь фантазией автора[264].

Отметим, что отделять субкультуры по внешнему виду, некоторым элементам терминологии, предпочтениям, видам деятельности (например, по направлениям музыки) не целесообразно. Во-первых, такой подход порождает огромное количество разнообразных субкультур, во-вторых описанные выше внешние элементы субкультур крайне динамичны и с течением времени сильно меняются. Основой разделения субкультур должен служить идеологический и ценностный базис.

Представляется, что преступная субкультура в Интернет идеологически и внешне крайне сходна с субкультурой хакеров и является ее частью. Скажем больше преступная субкультура в Интернет подвид субкультуры хакеров. При этом субкультура ха-

---

[262] Степанов-Егиянц В.Г. Преступления в сфере безопасности обращения компьютерной информации: сравнительный анализ: дис. ... канд. юрид. наук: 12.00.08. — М., 2005. — С. 40—41.

[263] Касперски К. Техника отладки программ без исходных текстов. — СПб.: БХВ-Петербург, 2005. — С. 24.

[264] Менжега М.М. Особенности установления личности хакера // Закон и право. — 2004. — № 8. — С. 62.

керов была изначально асоциальной, противопоставляя себя государству и обществу. Хотя на заре данного движения пропагандировалась бескорыстность, равенство и т.д., сейчас хакерские журналы и сайты просто пестрят информацией, как нелегально обогатиться. Хотя существуют преступники, которые действуют внешне бескорыстно, все равно в конечном итоге они получают выгоду[265]. Разговоры о бескорыстности компьютерных преступников следует оставить в 80-х, когда еще были сильны хакерские идеалы. Для современного Интернет-преступника хакерский идеал — это способ оправдания своих преступлений, получения прибыли и признания.

Нередко человек, который разделяет ценности хакера, готов на Интернет-преступление, либо одобряет преступления, совершаемые другими. Из всего вышесказанного можно сделать вывод, что *современная субкультура хакеров* по большему счету *имеет криминальную окраску*. Представляется, что необходимо отказаться от идеализации субкультуры хакеров и от мысли, что хакер не преступник.

Вообще разделение субкультуры хакеров, Интернет-преступников, компьютерных преступников, китайских хакеров, российских хакеров, вирусописателей и т.д. более чем условно, существует одна субкультура «хакеров», которая по-разному преломляется в различных субкультурных подгруппах или отражается согласно менталитету общества. Разграничить данные субкультуры можно было бы только в том случае, если различались бы совокупности их идей, ценностей, обычаев, традиций. Различия во внешних проявлениях говорят скорее о том, что это разные подвиды одной субкультуры, либо что это одна и та же субкультура в разное время. Заметим, что независимо от подгруппы меняется разве что интенсивность тех или иных проявлений, но все они присутствуют. То есть речь скорее идет о некоторых подтипах субкультуры хакеров, но не о новой субкультуре.

Изучение субкультуры хакеров не было бы так важно для развития Интернет-преступности, если бы она не выполняла множе-

---

[265] Например, распространители порнографии, которые не берут платы за данную продукцию, получают выгоду от распространения рекламы продуктов секс-индустрии. Или многочисленные сайты, распространяющие авторскую продукцию бесплатно, также получают выгоду в виде привлечения большого количества пользователей на свой сайт.

ство функций. В настоящее время существуют некоторые криминологические и социологические исследования[266], выделяющие функции негативных и преступных субкультур. Наиболее значимыми для Интернет-преступности, по нашему мнению, являются следующие.

Объединяющие. Тот факт, что хакеры по всему миру имеют схожие идеологические установки, взгляды на жизнь, способы заработка, используют одну и ту же литературу, термины и сленг, является мощнейшим объединяющим фактором. Хакеры могут легко объединяться в международные группы для совершения общественно опасных деяний, обмениваться профессиональной информацией и инструментами.

Легитимационные. Оправдание в глазах окружающих и соответствие своим морально-этическим установкам преступлений в Интернет дает дополнительный стимул для выбора криминального пути при достижении цели. Отсутствие явного общественного осуждения за подобное противоправное поведение приводит к парадоксальной ситуации, когда компьютерные преступники не только не скрываются, но и выставляют напоказ свои незаконные достижения, не боясь ответственности, оставляют фирменные знаки или лозунги[267] хакерских групп на местах преступлений. Кроме этого, как уже выше сказано, сами хакеры не называют свою деятельность преступной, что создает им романтический образ.

Информационные. Именно в рамках субкультуры распространяется идеологическая и инструментальная информация. В хакерской среде передаются новые способы и современные средства компьютерного взлома. Посредством своей субкультуры ха-

---

[266] Алоян А.А. Предупреждение распространения субкультуры наркомании в молодежной среде: дис. ... канд. юрид. наук: 12.00.08. — М., 2002. — С. 60—89; Денисов Н.Л. Влияние криминальной субкультуры на становление личности несовершеннолетнего преступника: дис. ... канд. юрид. наук: 12.00.08.— М., 2002. — С. 30—65; Павлова А.А. Субкультура теневой экономической деятельности: сущность и факторы воспроизводства в России: дис. ... канд. соц. наук: 22.00.03. — М., 2004. — С. 11—50; Тулегенов В.В. Криминальная субкультура и ее криминологическое значение: дис. ... канд. юрид. наук: 12.00.08. — Ростов-на-дону, 2003. — С. 45—113.

[267] Иногда сами хакеры по иронии называют это копирайтом. См.: Касперски К. Техника и философия хакерских атак — записки мыщ'а. — М.: СОЛОН-Пресс, 2004. — С. 22.

керы узнают, как уходить от правоохранительных органов и как уничтожить улики, какие методы добывания денег преступным путем наиболее безопасны и какие средства наиболее эффективны. Благодаря распространяемой в хакерской среде информации Интернет-преступники зачастую имеют техническое преимущество перед частными службами безопасности и государственными службами противодействия компьютерной преступности.

Криминогенная. Накопление, сохранение и передача традиций преступной Интернет-среды, которая способна противостоять социальным институтам. То есть обеспечение воспроизводства и распространения Интернет-преступности.

Представляется, что субкультура хакеров выполняет и другие функции, которые также связаны с угрожающей динамикой роста Интернет-преступности, но нами выделены наиболее значимые. Хакерская среда является основным и наименее исследуемым фактором, сопряженным с преступностью в Интернет. Данная преступная субкультура имеет свои особенности и в целом не похожа на общекриминальную российскую субкультуру; кроме того, хакерская среда является одним из главных криминогенных факторов Интернет-преступности, так как выполняет объединяющие, информационные, легитимационные функции. Представляется, что нейтрализация негативных последствий воздействия субкультуры хакеров является одной из первоочередных задач противодействия Интернет-преступности.

3.3. Детерминанты Интернет-преступности

П.С. Дагель писал, что эффективность предупреждения антиобщественных явлений прямо зависит от результатов теоретических исследований по выявлению причин и условий, порождающих преступные действия[268]. Компьютерная и Интернет-преступность, являясь частью всей преступности, подвержена влиянию причин и условий, свойственных для всей преступности в РФ[269]. Несмотря

[268] Дагель П.С. Причины преступности в СССР и причины индивидуального преступного поведения // Проблемы причинности в криминологии и уголовном праве. Межвузовский тематический сборник. — Владивосток: Изд-во Дальневост. ун-та, 1983. — С. 28.

[269] См.: Овчинников Б.Д. Вопросы теории криминологии. — СПб.: Изд-во Ленинградского ун-та, 1982. — С. 31 — 334 и др.

на это детерминанты компьютерной преступности и Интернет-преступности имеют существенные отличия, более того, и причины общие для всей преступности воздействуют на Интернет-преступность особым образом из-за свойств Глобальной сети и под влиянием субкультуры хакеров.

По мнению специалистов, появление компьютерной преступности свойственно всем государствам, которые в силу своего научного прогресса вступают в период широкой компьютеризации своей деятельности. При этом существенное влияние на динамику компьютерной преступности оказали возникшие в современном обществе противоречия между необходимостью свободного обмена информацией, расширения инструментария для этого, с одной стороны, и потребностями на введение ограничений на свободное использование определенных видов информации, — с другой[270].

Объясняя причины и условия возникновения, бурного роста Интернет-преступности, а также ее другие качества, мы придерживаемся широкого детерминистического подхода, когда преступность предстает как результат не однозначного влияния каких-то факторов, а сложной многоплановой детерминации, в том числе самодетерминации. Такой подход не только дает ответ на вопрос, почему существует преступность, но и почему она существует в настоящее время в настоящей форме[271].

Социально-экономические детерминации, общие для всей Российской преступности, в отношении компьютерной преступности приобретают совершенно другой характер. Во-первых, Россия страна с более низким уровнем жизни по сравнению со странами ЕС, США, некоторыми странами АТР и возможностями легального заработка. В свою очередь, сфера информационных технологий — это огромный теневой и криминальный рынок. Широкое распространение компьютерного пиратства определяется тем, что у населения и мелкого бизнеса нет средств на покупку дорогостоя-

---

[270] Кесареева Т.П. Криминологическая характеристика и предупреждение преступности в Российском сегменте сети Интернет: дис. ... канд. юрид. наук: 12.00.08. — М., 2002. — С. 113—114.

[271] Криминология: Учебник для вузов / Под общ. ред. д.ю.н. проф. А.И. Долговой. — 3-е изд. перераб. и доп. — М.: Норма, 2005. — С. 238.

щих легальных копий программ и поэтому спрос на дешевые нелегальные продукты очень велик[272].

Как считает М.С. Гаджиев, « ... компьютерная преступность — это проблема не полицейская и не правоохранительная, а проблема социальная. Как только уровень жизни повысится до определенного адекватного показателя, некоторые виды компьютерных преступлений исчезнут. Люди будут создавать себе меньше проблем, если будут покупать доступ в Интернет и лицензионные диски»[273]. С этим соглашается и Д.В. Добровольский, говоря о том, что существующее «цифровое» неравенство порождает дефицит компьютерной техники в странах с неразвитой компьютерной инфраструктурой. Лица, не имеющие доступа в Интернет, иной раз пытаются нелегально подключиться к Глобальной сети[274]. Мы отчасти согласны с этим мнением, так как определенная категория людей идет на преступления только по корыстным мотивам, из-за материальной невозможности пользоваться современными технологиями легально.

Представляется, что такой размах нарушения авторских и смежных прав действительно связан с недостаточно высокими доходами населения. Для России пиратство — это стратегический вопрос. Нелицензионные программы используются не только частными лицами, но и целыми организациями и учреждениями, в том числе государственными. Если предположить, что сегодня все пользователи перейдут на лицензионные программы, то расходы на информационное обеспечение вырастут многократно[275].

---

[272] Для сравнения — легальная копия Windows XP с минимальным набором функций стоит 8—9 тыс. руб., в свою очередь, нелегальный вариант — всего 100 руб. Также в Интернет появились целые порталы, предлагающие уголовно наказуемые услуги, — например, взлом электронной почты за деньги, при этом цена от 100 до 1000 руб. Небольшая плата за то, что можно читать практически всю корреспонденцию фирм конкурентов.

[273] Гаджиев М.С. Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан): дис. ... канд. юрид. наук: 12.00.08. — Махачкала, 2004. — С. 78.

[274] Добровольский Д.В. Актуальные проблемы борьбы с компьютерной преступностью: дис. ... канд. юрид. наук: 12.00.08. — М., 2005. — С. 55.

[275] Например, если даже половина российских пользователей компьютеров установит на свои компьютеры Windows средняя цена самой обычной конфигурации при покупке вместе с компьютером в среднем около 6000—7000 руб., то есть в масштабах страны приблизительно 300—350 млрд руб. Это только расходы на операционную систему без прикладных программ и в самой простой конфигурации «Номе» (для домашнего использования).

Например, Китай на государственном уровне «закрывает глаза» на некоторые виды интеллектуального «пиратства», хотя распространение незаконного копирования программных и технических средств там огромно. То, что представляет угрозу мировой экономике, не является внутренней проблемой отдельной страны. Китаю и другим развивающимися странам АТР просто необходимы новые программные продукты и средства, тогда как требования к соблюдению авторских прав скорее вопрос внешней политики[276]. Благодаря пиратству в области технологий Китаю во многом удалось выйти на высокий уровень развития компьютерной индустрии. Практически можно говорить, что данный вид компьютерного преступления молчаливо одобрен правительством. Как заявила администрация США, пиратство в России и Китае является открытым, хорошо известным и действующим без заметного противодействия со стороны правительств этих стран[277]. Защита авторских прав прежде всего выгодна странам с развитой отраслью информационных технологий.

Важно отметить, что корыстная мотивация не единственная даже в сфере таких преступлений, как доступ в Интернет за чужой счет. К тому же в Америке, где уровень жизни очень высок, а технологии гораздо дешевле, также отмечается очень высокий уровень использования нелегального программного обеспечения и доступа в Интернет в обход системы оплаты. Это свидетельствует о том, что увеличение дохода населения не решит проблему компьютерной преступности.

Компьютерные преступления приносят большие прибыли и несмотря на риск являются выгодным способом ведения деятельности. Распространение материалов посредством Интернет без учета авторских прав, порнография, сетевой терроризм, спам — все это является неотъемлемой частью мировой теневой и криминальной экономики[278]. Представляется, что некоторые отрасли Интернет-преступности давно выделились в самостоятельные при-

---

[276] Fan Gang. Piracy in China [Электронный ресурс] // Project Syndicate. — Режим доступа: http://www.project-syndicate.org/commentary/fang8

[277] Аркадий Орлов. Сенат США: Россия должна усилить защиту интеллектуальной собственности [Электронный ресурс] // РИА новости. — Режим доступа: http://www.rian.ru/world/america/20050427/39750675.html

[278] Кондратьев А. Порно, спам и пиратская музыка: кто и как зарабатывает на них в Интернете // Forbes. — 2006. — № 3 (март). — С. 47 — 54.

былые подвиды противоправной экономической деятельности (порнобизнес, нарушение авторских и смежных прав и т.д.). В этих секторах теневой и криминальной экономики в силу огромных средств задействованы наиболее технически грамотные специалисты, которые не могут получить достойной оплаты труда в легальных видах экономической деятельности.

Диктатура спекулятивного, теневого интереса в России неумолимо ведет к тяжелым криминальным проблемам. Сформировался слой миллиардеров, присваивающих сверхприбыль от спекуляции. В результате вести в России честный бизнес и заниматься законным предпринимательством невыгодно, что сказывается на экономической ситуации в стране[279]. Представляется, что рост и развитие Интернет-преступности приводит к возникновению новой экономической элиты, которая в будущем попытается влиять на экономические и политические процессы в стране.

При этом интеллектуальное развитие российских компьютерщиков явно превосходит в нашей стране скорость внедрения компьютерных технологий. Если по уровню компьютеризации Россия не входит и в двадцатку, а Интернет использует всего одна четвертая часть ее населения, то наши программисты считаются самыми лучшими в мире. Так, в 2000 — 2006 гг. российские программисты пять раз становились чемпионами мира по программированию и всегда находились в призерах не ниже второго места, при этом в двенадцать первых позиций каждый год входило, по меньшей мере, 3 команды россиян[280].

Несоответствие между развитием легального сектора экономики в области компьютерных технологий и способностями российских специалистов, заставляет наиболее высококвалифицированных из них нередко выбирать преступный путь и вовлекаться в теневую деятельность. Получается, что ценностные ориентации

---

[279] Демидов Р.С. Теневая экономика криминологический анализ: дис. ... канд. юрид. наук: 12.00.08. — М., 2002. — С. 101.

[280] The 30th Annual ACM-ICPC World Finals sponsored by IBM [Электронный ресурс] // The ACM-ICPC International Collegiate programming Contest. — Режим доступа: http://icpc.baylor.edu/icpc/Finals/Standings2006.html; Триумф российских студентов на чемпионате мира по программированию [Электронный ресурс] // ЦНТИ Прогресс. — Режим доступа: http://www.cntiprogress.ru/news/news_spb/2110.aspx

компьютерных специалистов подвергаются сильному давлению. С одной стороны, сейчас большой упор сделан на достижение нравственного благополучия, а с другой — трудно реализовать достижение этой цели законными путями.

Превосходство теневого сектора над легальным в сфере информационных технологий приводит к тому, что внутри российского рынка программного обеспечения программистам нет возможности получать прибыли с разработки собственных продуктов. Большинство фирм, разрабатывающих программное обеспечение, сориентированы на зарубежного покупателя. Несоответствие количества специалистов и рабочих мест приводит к оттоку интеллектуальной программистской элиты за границу или ее вовлечению в криминальные круги.

Нехватка рабочих мест в легальной экономике, связанная с неразвитостью сферы информационных технологий, является причиной роста компьютерной преступности, но получается, что неразвитость сферы технологий вычислительной техники во многом сама порождена компьютерной преступностью.

Выходит, что распространение незаконного программного обеспечения — причина сама в себе, то есть рост компьютерной преступности приводит к росту компьютерного «пиратства», а пиратство влечет за собой убыточность разработки компьютерных программ и не дает развиться сектору информационных технологий в России. Представляется, что и дороговизна компьютерных технологий, и несоизмеримость их стоимости с доходами также во многом обусловлены тем фактом, что Россия не производит своей компьютерной продукции и, следовательно, зависит от цены, устанавливаемой зарубежными производителями.

То есть многие условия и причины компьютерной преступности связаны с отсутствием достаточно развитой сферы информационных технологий. В свою очередь, одним из факторов, препятствующих развитию «компьютерной» экономики, является сама компьютерная преступность. Это одна из форм самодетерминации, которую мы обозначим как «социально-экономическую самодетерминацию». Социально-экономическая ситуация порождает компьютерную и Интернет-преступность, а они, в свою очередь, изменяют социально-экономическую ситуацию, что приводит к дальнейшему изменению компьютерной и Интернет-преступности.

Несмотря на то, что на Интернет-преступность сильно влияют общие для всей компьютерной преступности детерминанты, заметим, что Интернет-преступность имеет целый комплекс своих специфичных детерминант. Среди них необходимо выделить появление такого явления, как Глобальная информационная сеть. Создание Интернет предопределило возникновение новых видов общественных отношений. Ведь без существования Интернет невозможна Интернет-преступность.

Так, например, А.А. Жмыхов выделяет три особенности Интернет, которые способствуют совершению преступлений. Во-первых, виртуальная среда Глобальной сети предоставляет преступнику анонимность, так как фактически он находится в реальном мире, а совершает преступления в виртуальном. Во-вторых, преступника и жертву разделяют сотни, а иногда и тысячи километров. В-третьих, компьютерная среда обеспечивает лучшее, по сравнению с традиционными средствами, качество предоставления информации[281].

М.С. Гаджиев считает, что стремительное развитие телекоммуникаций и глобальных компьютерных сетей создало условия, облегчающие совершение преступлений в сфере высоких технологий. В настоящее время многие традиционные преступления невозможно совершать или масштабно, или без риска быстрого разоблачения, если не использовать высокие технологии[282].

Свойства Глобальной сети Интернет действительно делают преступления более безопасными, эффективными и легкими для преступника и способствуют быстрому росту такой молодой преступности, как Интернет-преступность. Представляется, что для установления причин роста, порожденных самой Глобальной сетью, необходимо внимательно рассмотреть свойства самого Интернет не только как технологии, но и как культурного, социально-экономического, правового и политического явления.

Появлявшиеся новые технологии, такие как изобретение автомобиля, телеграфа, телефона, давали не только мощный толчок

---

[281] Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение: дис. ... канд. юрид. наук: 12.00.08. — М., 2003. — С. 38.

[282] Гаджиев М.С. Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан): дис. ... канд. юрид. наук: 12.00.08. — Махачкала, 2004. — С. 87—88.

прогрессу, но и создавали определенные преимущества для преступной деятельности. Несмотря на тот факт, что сеть с точки зрения Интернет — это всего лишь современная технология, отметим, что ни одна технология до этого не давала таких преимуществ преступникам и не была так неподконтрольна законам, как Интернет в силу принципов и правил, определяющих ее функционирование. Некоторые особенности Глобальной сети отличают ее от предшествующих технологий и требуют новых методов борьбы с порождаемой ею преступностью. Именно эти особенности и способствуют росту некоторых видов Интернет-преступности.

Во-первых, Интернет имеет *глобальную трансграничную природу*, что вызвано архитектурой самой сети. Это способствует развитию и росту всей Интернет-преступности, независимо от подвидов. Интернет позволяет совершать преступления на территории другого государства с домашнего компьютера. Кроме этого, Глобальная сеть способствует кооперации и консолидации международных преступных группировок и сообществ независимо от вида деятельности[283].

Во-вторых, одним из принципов Интернет-технологии является *анонимность*, что, в первую очередь, обеспечивает преимущества для всех форм мошенничества и обмана. Не только обман с целью завладения денежными средствами, но и обман с политическими целями. Так, например, возможность анонимной публикации информации в Интернет активно используют для нечестной предвыборной борьбы с конкурентами.

Вообще анонимность позволяет публиковать информацию любого свойства с минимальным риском понести уголовную или иную ответственность. Анонимность дает преимущества не только в размещении преступной информации, но и влияет на увеличение спроса на нее. Так, общественно осуждаемая детская порнография, может анонимно просматриваться педофилами без угрозы огласки. Выходит, что анонимность Интернет создает устойчивый спрос на информацию преступного характера.

---

[283] Например, Интернет не только позволяет создавать международные хакерские группировки для совершения преступлений в сфере компьютерной информации, но дает преимущества для создания международных террористических групп с целью консолидации распространителей порнографии, организации наркотрафика и т.д.

В-третьих, Интернет имеет огромный потенциал для *охвата широкой аудитории*, делая возможным совершать беспрецедентные по количеству пострадавших-потерпевших от преступления. Использование Интернет в преступлениях зачастую позволяет многократно увеличить вред, наносимый общественно опасным деянием, по сравнению с тем, что совершалось без использования Глобальной сети. Порнографическая продукция, компьютерные вирусы, призывы к совершению экстремистских, националистических, террористических преступных действий, реклама наркотиков — все это может успешно распространяться на неопределенно большую аудиторию Интернет.

В-четвертых, сложности в борьбе с преступностью и правовом регулировании Интернет, что дает определенные преимущества преступникам, использующим Глобальную сеть, создает *распределение основных узлов сети и их взаимозаменяемость*. Дело в том, что когда создавалась сеть ARPANet (Advanced Research Project Agency network) — прообраз Интернет, в нее была заложена возможность функционирования при выходе из строя нескольких ключевых узлов, дающая преступникам несколько преимуществ. В первую очередь, — это возможность при перекрытии одного канала информации передавать его по альтернативному, что делает очень сложным полный контроль потоков информации в Глобальной сети[284].

Кроме этого, распределение трафиков, когда каждое подключение идет по многим каналам, приводит к тому, что улики совершения того или иного Интернет-преступления затем придется собирать по всему миру, по разным странам и континентам[285].

Исходя из вышеизложенного полагаем, что в отличие от компьютерной преступности, которая мало чем отличается от другой преступности, выделенной по средству совершения, появление Интернет в том виде, в котором он существует, без учета многих юридических моментов и, давая беспрецедентные возможности

---

[284] Например, в Китае заявлено, что контролируется весь внешнегосударственный Интернет-трафик, — что не мешает китайским хакерам атаковать компьютеры по всему миру. Если преступнику перекрыть один канал, то зачастую можно найти другой без ущерба для осуществляемой деятельности.

[285] См. например: Волеводз А.Г. Следы преступлений, совершенных в компьютерных сетях // Российский следователь. — 2002. — № 1. — С. 6.

преступнику, является одной из основных детерминант Интернет-преступности. То есть широкая распространенность, структура, высокая общественная опасность Интернет-преступности во многом обусловлены свойствами сети. Интернет влияет на многие факторы и параметры Интернет-преступности. Например, такое широкое распространение идеологии Интернет-преступников невозможно без существования Интернет.

Несмотря на то, что большинство причин быстрого роста и распространенности Интернет-преступности заложено в принципах и протоколах самой технологии, необходимо отметить, что в настоящее время Глобальная сеть — это не просто технология, а уникальное социальное, культурное, экономическое и правовое явление.

Интернет как социальное явление получил очень широкую распространенность. В настоящее время количество пользователей Интернет в мире и в России стремительно увеличивается, возрастает и число потенциальных преступников в Глобальной сети. При этом вряд ли существует линейная корреляция роста числа пользователей и роста Интернет-преступности. Так, например, в США количество пользователей Интернет выросло с 2002 по 2005 гг. на 2,7%[286], тогда как по данным центра исследования компьютерной преступности CERT количество зарегистрированных хакерских атак только в 2003 г. выросло на 66,5%[287].

В России за 2003-2005 гг. прирост количества зарегистрированных преступлений в сфере компьютерной информации и числа ее пользователей примерно равны. В 2005 г., по сравнению с 2004 г., количество уголовно запрещенных деяний в сфере компьютерной информации выросло на 16,9%. А рост пользователей Глобальной сети в России составил около 19%. Такие же данные получены при сравнении 2003 г. с 2004 г. Но делать выводы о прямопорциональном росте Интернет-преступности и количества пользователей Интернет не следует в силу искажения реального числа преступлений, совершенных в Глобальной сети, из-за высокой латентнос-

---

[286] Россия получила «бронзу» за рост компьютеризации [Электронный ресурс] // CNEWS.ru. — Режим доступа: http://www.cnews.ru/news/top/index.shtml —2006/03/02/197072

[287] CERT/CC Statistics 1988-2006[Электронный ресурс] // CERT. — Режим доступа: http://www.cert.org/stats/cert_stats.html

ти Интернет-преступности. Тем более, последние годы (2006 — 2007 гг.) наблюдается снижение регистрируемых преступлений в сфере компьютерной информации, а количество российских Интернет-пользователей растет.

Социально-экономические детерминанты. Мы не будем описывать такие общие для всей преступности детерминанты, как имущественное расслоение общества, кризис экономики, безработицу и т.д., так как данные детерминанты давно изучены и их влияние на Интернет мало чем отличается от воздействия на другие виды преступности. Прежде всего, необходимо выделить детерминанты, свойственные только Интернет-преступности, либо свойственные и другим видам преступности, но с другим характером воздействия.

Интернет дает возможность найти заработок по всему миру. Это подтверждает и рассмотрение подпольного рынка Интернет-порнографии. Зарплата девушки, работающей на портале live-cam[288] порнографии, составляет от 1$ и более в минуту, при этом ей не надо вступать в физический контакт, совмещая такую виртуальную деятельность с учебой или какой-либо вполне легальной работой. Порномодель зарабатывает от 200 долларов США в день (что равнозначно 5 — 6 тыс. руб. — ежемесячной зарплате многих российских граждан). Клиентами этих порталов чаще всего являются иностранцы[289].

Из-за огромных финансовых возможностей нелегального заработка, сосредоточенных в Интернет, наиболее активно развиваются виды преступлений, направленных на извлечение прибыли, таких как распространение Интернет-порнографии, спама (во многих странах спам криминализован), нарушение авторских и смежных прав, Интернет-мошенничество. Представляется, что это наиболее быстро развивающиеся отрасли Интернет-преступности. Более того, Интернет-порнография и спам дали жизнь множе-

---

[288] Live cam — вид порно-услуг, когда клиент наблюдает за моделью посредством удаленной Интернет-камеры и говорит, какие действия интимного характера ей с собой сделать.

[289] Голубев В.А. Доходы от детского порнобизнеса превышают доходы колумбийской наркомафии [Электронный ресурс] / Центр исследования компьютерной преступности. — Режим доступа: http://www.crime-research.ru/analytics/gol100207/; Твоя порностудия // Хакер. — 2004. — № 6 (66). — С. 52.

ству новых технологий, то есть это наиболее технологически развитые виды преступности.

Все финансовые потоки в нелегальных видах Интернет-бизнеса скрыты от государства благодаря появлению такого феномена, как Интернет-деньги. В мире в последнее время появилось много всевозможных денежных Интернет-систем: PayPal (от pay palace — дворец оплаты), eGold (от electronic Gold — электронное золото), WebMoney (рус. — сетевые деньги) и RuPay (от Russian Pay — русская оплата) и т. д. Чтобы создать счет в подобной системе, не нужно ни паспорта, ни каких-либо других идентификационных документов[290]. Паспорт требуется при вводе денег в платежную систему или выводе из нее, а все перемещения со счета на счет внутри осуществляются через Интернет. То есть любой человек, имеющий доступ в Интернет, может открыть счет в такой системе, не выходя из дома, при этом указав какие-угодно персональные данные. Это приводит к тому, что огромные денежные потоки остаются «в тени», без социального и правового контроля.

Кроме того, чтобы перевести деньги из одной системы в другую или переместить через границу, также не нужно каких-либо документов. Это обеспечивается при помощи так называемых частных обменных пунктов. При комиссии около 10% можно перевести абсолютно анонимно деньги из одной системы в другую и через границу в течение суток. Используя подобные схемы, ввозят деньги в страну владельцы зарубежных порносайтов и мошенники, действующие в России.

Теневой поток денег в Интернет стимулирует развитие преступности, особенно с корыстной мотивацией. Представляется, что хотя теневые финансовые потоки существуют и в других видах преступности, но обычно легализация — это сложный и дорогостоящий процесс, а не результат нажатия нескольких кнопок на клавиатуре. Развитие теневой экономики в сети Интернет, в том числе огромные бесконтрольные потоки, приводят к росту количества вовлеченных в этот процесс.

Социально-политические детерминанты. Отсутствие каких-либо границ в Глобальной сети и трудность в согласовании дей-

[290] Хотя в американской системе Paypal требуются реально существующий телефон и адрес, эти данные можно легко достать в Интернет, не пользуясь какими-либо преступными ухищрениями.

ствий в области борьбы и профилактики Интернет-преступности, различия позиций по отношению к свободе слова, аморальной информации, разница в оценках тех или иных действий в различных государствах приводит к сетевой анархии, невозможности правового регулирования сети, сводят на нет усилия правоохранительных органов.

Недовольство политическим устройством и внешнеполитическим курсом России подталкивает некоторых преступников к активным действиям. Например, бездействие российских властей по поводу притеснения русскоязычных жителей прибалтийских стран привело к неоднократным атакам русских хакеров на официальные сайты учреждений этих государств. Также активно участвовали российские Интернет-преступники в сетевых атаках во время вооруженного конфликта в Косово[291]. Заметим, что Интернет позволяет любому пользователю участвовать в политических событиях по всему миру, а при наличии определенных технических навыков даже влиять на эти события.

Роль политического противоборства в генезисе современной преступности изучена совершенно недостаточно. Хотя политические интересы в большинстве своем связаны с борьбой за власть, в процессе которой в выборе средств политические антиподы не очень-то церемонятся[292].

Представляется, что компьютерная и Интернет-преступность результат борьбы новой экономической элиты с властью ТНК и государств, передела сфер влияния на информационные и финансовые потоки. При этом новая «информационная элита» категорически не признает права обладания информацией за государством и корпорациями. В таких областях, как нарушение авторских и смежных прав, Интернет-порнография и спам сосредоточены огромные организационные и финансовые ресурсы, превосходящие доходы наркокартелей, они могут влиять не только на внутригосударственную, но и мировую политику.

Социокультурные детерминанты. Субкультура хакеров является сильным фактором, объединяющим Интернет-преступников

---

[291] См: http://buro-dv.ru/public/kraushkin/kr_1.htm; http://gazeta.lenta.ru/daynews/16-06-1999/15hackers_Printed.htm; http://www.nabat.info/article.php?content_id=120

[292] Криминология: Учебник / под. ред. В.Н. Бурлакова, Н.М. Кропачева. — СПб.: Санкт-Петербургский гос. ун-т., 2002. — С. 102.

по всему миру. Имея одни идеологические установки, сленг, предпочтения, хакеры легко объединяются в группы, обмениваются опытом и специальными компьютерными программами. Субкультура хакеров является одним из самых мощных факторов воспроизводства сетевой преступности.

Субкультура хакеров разрекламирована через СМИ и Интернет. Образ компьютерного преступника сильно идеализирован и приветствуется среди молодежи. При этом к идеализации склонны не только не сведущая в компьютерах общественность и молодежь, но и многие компьютерные специалисты. Так, например, Джерри Ли Форд говорит, что хакеры просто компьютерные профессионалы и не больше — их мастерство не позволяет им идти на преступления. А те, кто совершает противозаконные деяния, обладают гораздо меньшим профессионализмом и их знания даже близко не равны умениям настоящего хакера[293].

К сожалению, количество компьютерных гениев-преступников так велико, что вряд ли можно назвать данное утверждение правдой. Например, исключительные компьютерные знания не мешали Кевину Митнику, хакеру номер один, как его называют (и другим хакерам из 10-ки самых знаменитых), совершать целые серии преступных деяний. Выходит, что субкультура хакеров это своеобразное продвижение образа жизни и ценностей компьютерного преступника в широкие массы; реклама, делающая преступный путь привлекательным и популярным. Так, Н.Н. Лебедева считает, что под влиянием контркультур (субкультур) общество и правовые системы стали более либеральными по отношению к различного рода девиациям, таким как наркомания, гомосексуализм и др.[294]

Субкультура хакеров оказывает особое влияние на лиц с несформировавшимися культурно-ценностными ориентирами. Помнению, М.М. Бабаева, противоправное поведение молодежи принято рассматривать как следствие проникновения в эту среду криминальной субкультуры[295]. Субкультура хакеров, в свою очередь,

---

[293] Джерри Ли Форд. Персональная защита от хакеров. Руководство для начинающих. Пер. с англ. — М.: КУДИЦ-ОБРАЗ, 2002. — С. 21—22.

[294] Лебедева Н.Н. Правовая культура личности и Интернет (Теоретический аспект): дис. ... канд. юрид. наук: 12.00.01.— М., 2004. — С. 81—82.

[295] Бабаев М.М. Социально-психологические компоненты детерминации преступного поведения молодежи // Российский криминологический взгляд. — 2005. — № 1. — С. 65.

не только позволяет оправдать совершение преступлений, но и провозглашает компьютерные преступления не преступным актом. При этом популярность молодежных субкультур позволяет им эффективно противостоять уже устоявшимся институтам социализации, — таким как школа, семья.

Представляется, что влияние данной преступной субкультуры усилилось благодаря всеобщей деморализации и деидеологизации общества. Например, Н.В. Ильина отмечает, что социально-психологический кризис в обществе привел к образованию определенного слоя людей, не имеющих криминального прошлого, но психологически готовых к совершению преступления, даже тяжкого[296].

Заметим, что компьютерные и Интернет-преступники это, как правило, люди трудолюбивые, доказавшие свои способности в области компьютерных технологий и созидательной деятельности в написании программ взлома. Несмотря на реальную возможность самореализации в рамках закона, они выбирают преступный путь под влиянием хакерской среды, которая апеллирует к таким человеческим ценностям и потребностям, как стремление к свободе, равенство вероисповедания и рас, тяга к знаниям и др.

Во многом это связано, с феноменом, который условно называют «патологией самовыражения», что является следствием современной «бездуховности» молодежи. Наблюдается стремление выразить себя в поступке, проявить свое «я» даже вопреки общепринятым мнениям и правилам поведения, нередко вопреки собственным интересам и безопасности, — все это во все времена было свойственно и остается таковым для людей молодежного возраста[297]. Именно на эту благодатную почву ложатся ценности таких заимствованных за рубежом деструктивных молодежных субкультур, как хакеры.

---

[296] Ильина Н.В. Особенности причинного комплекса преступности в условиях перехода к рыночной экономике: дис. ... канд. юрид. наук: 12.00.08. — М., 1998. См. также: Шестаков Д.А. Преступность как свойство общества. — СПб.: Изд-во «Лань», 2001. — С. 119—120; Шнайдер Г.Й. Криминология: Пер. с нем. / Под общ. ред. с предисл. Л.О. Иванова. — М.: Издательская группа «Прогресс»-«Универс», 1994. — С. 279—283.

[297] Бабаев М.М. Лекция по теме: феномены молодежной преступности // Российский криминологический взгляд. — 2007. — № 2. — С.114.

Отметим, что, несмотря на «импортированный характер» субкультуры хакеров, нельзя не сказать также о культурных отличиях российского компьютерного преступника, которые определяют характеристики Интернет-преступности в России и ее отличие от мировой преступности в Глобальной сети.

Российский тип хакеров обусловлен общими чертами культурного развития нашей страны. М. Вершинин выделил следующие отличия:

- неопределенность самосознания и поиск культурной идентичности;
- бинарный характер существования и развития культуры;
- коллективизм сознания, отрицающего иерархию;
- отношение к власти и законам как внешнему, чуждому элементу;
- установка на восприятие руководителя государства как защитника народа и противопоставление его бюрократическим структурам.

Русские хакеры в большей степени предрасположены к идеологическому обоснованию взломов, чем их собратья за рубежом[298]. Примерами служат взлом сайта ФБР во время бомбежек Югославии; критика деятельности «Microsoft», выпускающей на рынок некачественную с точки зрения информационной безопасности продукцию; взлом чешских сайтов в связи с размещением там радара НАТО. Взлом сайтов и программ часто осуществляется без получения выгоды, в целях демонстрации имеющихся недостатков в системе безопасности. Представляется, что это свидетельствует о широкой распространенности среди русских хакеров мотивации, отличной от корыстной.

Другой аспект — это пропаганда не хакерской, а общекриминальной субкультуры или ее отдельных подвидов. Данная проблема практически не привлекает внимания криминологов. В Глобальной сети практически беспрепятственно формируется и пропагандируется криминальная идеология, обеспечивается обмен опытом участников преступлений. Некоторые криминальные авторитеты в России создают собственные вебсайты[299]. Получается, что бес-

---

[298] Вершинин М. Современные молодежные субкультуры: хакеры [Электронный ресурс] / "Пси фактор" Центр практической психологии. — Режим доступа: http://www.psyfactor.org/lib/vershinin4.htm

[299] См: Номоконов В.А. Глобализация информационных процессов и преступность // Інформаційні технології та безпека. — Киев, 2002. — С. 97.

контрольное распространение информации в Интернет является условием, способствующим росту всей преступности в РФ.

Было бы явным упрощением считать, что колоссальный объем российской теневой и криминальной экономики возможен вне всякой связи с культурно-ценностной приемлемостью этого явления. Россияне отдают предпочтение неформальной экономике не только в связи с материальной стороной вопроса. Во многих странах Центральной и Восточной Европы рыночные реформы сопровождались обнищанием, безработицей, но при схожих условиях масштаб экономики в тени сильно различается, что во многом определяется нравственными установками, в том числе ценностными, так как российский гражданин во все времена противопоставлял себя официальной власти[300]. При этом некоторые меры, предпринимаемые властью, только усиливают недоверие к ней. Так, показателен пример суда над директором Пермской школы[301], который использовал нелицензионное программное обеспечение, хотя пиратские программные продукты используются повсеместно, в том числе и в структурах самой власти.

Представляется, что особенность причин, свойственных только для Интернет-преступности, подчеркивает ее отличие от других видов преступности, поэтому при разработке мер борьбы и профилактики, направленных на борьбу с преступностью в сети, необходимо учитывать эти исключительные характеристики. Более того, для эффективного противодействия могут потребоваться методы ранее не используемые, либо используемые в другом качестве совместно с уже давно опробованными.

Детерминанты уголовно-правового характера. Как было отмечено выше, в связи с быстрым ростом количества преступлений и усложнением структуры Интернет-преступности законодатель зачастую не успевает ответить на все вызовы, брошенные Интернет-технологией. С каждым годом появляются все новые

---

[300] Барсукова С.Ю. Неформальная экономика: структура и функциональная специфика элементов: дис. ... докт. соц. наук: 22.00.03. — М., 2004. — С. 141.

[301] Директора пермской школы могут осудить за использование нелицензионного Windows [Электронный ресурс] // Российский общеобразовательный портал. — Режим доступа: http://region.edu.ru/perm/news.asp?ob_no=7861

виды общественно опасной Интернет-деятельности, которые обладают признаками преступлений, но еще не криминализованы.

Традиционные преступления, совершавшиеся ранее без использования сети, выходят на новый качественный уровень, преступность во многом благодаря Интернет стала еще более транснациональной и межгосударственной. Несовершенство правовых норм или их полное отсутствие в сфере борьбы с Интернет-преступлениями видится нам одной из причин быстрого роста преступности в русскоязычной Глобальной сети.

Например, С.Д. Бражник утверждает, что в настоящее время становится все более очевидным тот факт, что ныне действующее уголовное законодательство не позволяет эффективно бороться с преступлениями в сфере компьютерной информации. Существующее информационное законодательство России также не свободно от недостатков, во многом оно декларативно и противоречиво. Изложенное приводит к многочисленным правовым ошибкам и принятию неверных судебных решений[302].

В.В. Воробьев считает, что практика применения уголовного законодательства свидетельствует о том, что возникающие в процессе борьбы с компьютерной преступностью проблемы обусловлены несовершенством уголовно-правовых норм, противоречивостью их толкования, отсутствием научно-методических рекомендаций и официальных руководящих разъяснений по квалификации этих деяний[303].

О противоречивости российского уголовного законодательства в формулировках уголовно-правовых норм, которая отрицательно сказывается на эффективности применения, говорит Т.Г. Смирнова[304]. Соглашаясь с перечисленными замечаниями, необходимо отметить, что не только непродуманность и противоречивость существующих норм способствует росту Интернет-преступности, но

---

[302] Бражник С.Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: дис. ... канд. юрид. наук: 12.00.08. — Ижевск, 2002. — С. 4.

[303] Воробьев В.В. Преступления в сфере компьютерной информации (юридическая характеристика и квалификация): дис. ... канд. юрид. наук: 12.00.08. — Нижний Новгород, 2000. — С. 5.

[304] Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: дис. ... канд. юрид. наук: 12.00.08. — М., 1998. — С. 133.

также тот факт, что многие общественно опасные деяния, обладающие необходимыми признаками для их криминализации, до сих пор не криминализованы.

Наиболее часто применяемыми статьями при квалификации Интернет-преступлений в России являются ст. ст. 272 и 273 УК РФ. При этом в настоящее время существует множество научных работ, в которых говорится о недостаточной проработанности данных составов[305].

Объединяя обсуждаемые в специальной юридической литературе проблемы современной редакции ст. 272 УК РФ, можно выделить наиболее значимые из них:

- данная норма носит бланкетный характер, следовательно, целесообразно ввести более полный перечень положений, закрепленных в иных законодательных документах, в частности, в законах «Об информации, информатизации и защите информации», «О государственной тайне» и др.;

- различия в трактовке терминов «неправомерный доступ», «информация»;

- законодатель для неправомерного доступа (ст. 272 УК РФ) не предусмотрел такого квалифицирующего признака, как совершение деяния группой без предварительного сговора, хотя специалисты признают, что это нередко встречается. А также уровнял преступления, совершенные «группой лиц по предварительному сговору» и «организованной группой»;

- законодатель не разграничил тяжесть преступлений исходя из ценности информации, к которой получен доступ.

---

[305] См: Бражник С.Д. Преступления в сфере компьютерной информации: проблемы законодательной техники; Бытко С.Ю. Некоторые проблемы уголовной ответственности за преступления, совершаемые с использованием компьютерных технологий; Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия; Воробьев В.В. Преступления в сфере компьютерной информации (юридическая характеристика и квалификация); Геллер А.В. Уголовно-правовые и криминологические аспекты обеспечения защиты электронной информации и Интернета; Доронин А.М. Уголовная ответственность за неправомерный доступ к компьютерной информации; Быков В., Нехорошев А., Черкасов В. Совершенствование уголовной ответственности за преступления сопряженные с компьютерными технологиями, Числин В.П. Уголовно-правовые меры защиты информации от неправомерного доступа: Середа С.А., Федотов Н.Н. Сложности толкования терминов «вредоносная программа» и «неправомерный доступ» и др.

Статья 273 УК РФ также имеет ряд пробелов, например:

- до сих пор не было приведено каких-либо аргументов в пользу того, что деяние, предусмотренное ст. 273 УК РФ, представляет какую-то чрезвычайную угрозу или особую опасность, требующую исключения из общих принципов криминализации. Не подтверждается и тезис о том, что «при использовании вредоносных программ вред наступает неминуемо»[306]. Этот факт ставит под сомнение целесообразность криминализации данного деяния;

- термин «создание, использование и распространение вредоносных программ для ЭВМ» достаточно емок и охватывает деяния, не содержащие признаков преступлений, как, например, запись исходного кода вируса на листе бумаги.

Кроме этого нельзя не отметить общие ошибки, допущенные в Главе 28 УК РФ, это:

- механическое перенесение в сферу права узкотехнических понятий и терминов из области информационных технологий, где их адекватность и целесообразность не вызывают сомнения;

- использование технических категорий типа «блокирование», «копирование», «модификация» и оценочных категорий «существенный вред», «тяжкие последствия», а не апробированных многолетней практикой стоимостных критериев: «значительный ущерб», «крупный» и «особо крупный размер».

Эти и некоторые другие недоработки в формулировке и толковании закона порождают сложности в уголовно-правовой практике борьбы с Интернет-преступлениями. Трудности в привлечении к уголовной ответственности являются серьезным стимулом как для совершения конкретных преступлений, так и для роста всей Интернет-преступности в целом. Низкий уровень раскрываемости компьютерных преступлений (в т.ч. Интернет-преступлений) формирует у будущих преступников ощущение безнаказанности. Многие из преступников никогда не совершали бы «обычных» преступлений из-за боязни наказания[307]. В свою очередь, Интернет-преступники хорошо осведомлены о недостатках российского за-

---

[306] Кругликов Л.Л. Практикум по уголовному праву. Общая часть. Особенная часть: Учебное пособие. — М,: Бек-Москва, 2002. — С. 275.

[307] Бытко С.Ю. Некоторые проблемы уголовной ответственности за преступления, совершаемые с использованием компьютерных технологий: дис. ... канд. юрид. наук: 12.00.08. — Саратов, 2002. — С.90.

конодательства благодаря широко распространенной субкультуре хакеров.

Особенно чувство безнаказанности присуще при совершении чисто компьютерных преступлений, квалифицируемых по статьям Главы 28. Например, проведенное К.Н. Евдокимовым исследование показало, что 40% опрошенных пользователей ЭВМ готово проникнуть в чужую систему и ознакомиться с информацией, если об этом никто не узнает[308]. Это связано с несформировавшейся правовой культурой в области новых для общества отношений и прямым поощрением подобного поведения определенными субкультурными группами.

Представляет угрозу и хакер, уже совершивший преступление; в случае занятия им ключевой должности в сфере компьютерных технологий велика вероятность того, что в силу асоциальных установок, сформированных субкультурой хакеров, Интернет-преступник может повторно нарушить закон. Выходит, что преступник, склонный к компьютерному взлому, может получить доступ к системам ЭВМ коммерческого, промышленного и государственного значения. В США, например, лишение права заниматься деятельностью в области компьютерных технологий для преступников, совершивших компьютерные преступления, стало одной из самых часто применяемых мер наказания.

Так, известному хакеру Кевину Митнику после отбытия первого наказания было запрещено работать в компьютерной индустрии в течение трех лет[309]. В УК РФ лишение права занимать определенные должности или заниматься определенной деятельностью относится к видам применяемого наказания, но не используется в статьях Главы 28 «Преступления в сфере компьютерной информации».

Представляется, что отсутствие данного вида уголовного наказания в составах Главы 28 открывает лицам, совершившим компьютерные преступления и имеющим склонность совершать по-

---

[308] Евдокимов К.Н. Уголовно-правовые и криминологические аспекты противодействия неправомерному доступу к компьютерной информации: дис. ... канд. юрид. наук: 12.00.08. — Иркутск, 2006. — С.139.

[309] Kevin Mitnick sentenced to nearly four years in prison [Электронный ресурс] / Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice. — Режим доступа: http://www.cybercrime.gov/mitnick.htm

добные деяния, новые возможности в работе с важными системами ЭВМ в России, позволяют в дальнейшем совершать еще более тяжкие преступления. По нашем мнению, данный серьезный пробел должен быть восполнен внесением соответствующего дополнения в УК РФ.

Кроме недостаточной продуманности существующей системы мер уголовного воздействия, существенной причиной роста преступности является отсутствие в уголовном кодексе статей, предусматривающих ответственность за некоторые деяния, криминализация которых уже давно необходима. Например, спам (критерии криминализации рассмотрены в § 3.2) не только стал угрозой функционирования всего Интернет, но и является серьезным экономическим подспорьем преступности в Глобальной сети. Спамеры зачастую оплачивают Интернет-преступникам совершение тех или иных общественно опасных деяний. Кроме того, спам приносит огромный материальный, технический и моральный ущерб как в масштабе отдельно взятого государства, так и мирового сообщества в целом.

Представляется, что причины и условия уголовно-правового характера не только влияют на рост Интернет-преступности, но серьезно снижают эффективность уголовно-правовой борьбы с преступностью в Глобальной сети. Выходит, что правовые факторы наряду с субкультурными и социально-экономическими являются также весомыми, обуславливающими существование и дальнейшее распространение Интернет-преступности.

3.4. Меры предупреждения и борьбы с Интернет-преступностью

Основной целью криминологического исследования считается разработка научно обоснованных и практически значимых мер воздействия на преступность, а также оценка существующих. Именно предложение способов предупреждения и борьбы с Интернет-преступностью является логичным результатом проделанной работы. Подход к преступности как к социально-негативному явлению предполагает соответствующую стратегию борьбы с нею в рамках государственной уголовной политики, главным направлением в которой является воздействие на порождающие ее причины.

В криминологии предупреждением преступности принято считать многоуровневую систему государственных и общественных мер, направленных на выявление, устранение, ослабление или нейтрализацию причин и условий преступности, её отдельных видов и конкретных деяний, а также на удержание от перехода или возврата на преступный путь людей, условия жизни и (или) поведение которых указывает на такую возможность[310].

Общим объектом предупреждения преступности являются условия и причины преступлений и преступности, а именно криминогенные социальные явления, обуславливающие виды, состояние и динамику преступности, а также негативные воздействия на микроуровне.

По направленности и видам (содержанию) специалисты выделяют такие меры профилактики на всех её уровнях, как социально-экономические, организационно-управленческие, идеологические, социально-психологические, медицинские, психолого-педагогические, технические, правовые, культурно-воспитательные и иные (например, экологического, демографического характера)[311].

Учитывая детерминирующие факторы и условия Интернет-преступности, мы подробно раскроем лишь организационные, технические, экономические и идеологические меры и отдельно — правовые меры предупреждения и борьбы с Интернет-преступностью.

Организационные меры предупреждения Интернет-преступлений принимаются для структурирования работы и взаимодействия органов государственной власти, принятия различных решений по надзору за деятельностью Интернет и информацией, распространяемой не её порталах. Выделение вопроса общей организации предупреждения преступлений в Глобальной сети служит предпосылкой для решения вопросов об определении круга

---

[310] Криминология: учебник для студентов вузов / Под науч. ред. Н.Ф Кузнецовой, В.В. Лунеева. — М.: Изд-во Волтерс Клувер, 2005. — С. 185.

[311] Криминология: Учебник для вузов / Под общ. ред. д.ю.н. В.Н. Бурлакова. — СПб.: Изд-во Питер, 2002. С. 182—183; Криминология: Учебник / Под ред. В.Н. Кудрявцева, В.Е. Эминова. — 2-е изд — М.: Юристъ, 1999. — С. 286—288; Криминология: учебник для студентов вузов / Под науч. ред. Н.Ф Кузнецовой, В.В. Лунеева. — М.: Изд-во Волтерс Клувер, 2005. — С. 197—200; Терещенко Б.Л. Предупреждение преступлений, посягающих на интеллектуальную собственность: дис. ... канд. юрид. наук: 12.00.08. — М., 2005. — С. 119.

субъектов, занимающихся этой деятельностью, механизма их взаимодействия, полномочиях и др.

Камнем преткновения является следующий вопрос: кто должен играть ключевую роль в регулировании информации, а, следовательно, и в предупреждении преступлений в сети Интернет, — государственные структуры, гражданское общество, отдельные общественные организации или отраслевые структуры? Согласно нашим исследованиям, профессионалы в компьютерных технологиях считают, что преобладать должен личный контроль (около 64%), то есть каждый может получать доступ к любой информации и сам выбирать, какая приносит ему вред, а какая нет. В свою очередь, примерно равное количество опрошенных нами респондентов — специалистов в компьютерных технологиях признает, что одним из главных должен быть либо отраслевой (27,56%), либо государственный (24,41%), либо общественный контроль (24,41%).

Несмотря на то, что это мнение специалистов в области Интернет-технологий, мы вынуждены с ними не согласиться. Такая точка зрения связана с тем, что компьютерные профессионалы фактически обладают квалификацией такого уровня, что способны самостоятельно оградить себя от незаконной и вредной для них информации, а также воспрепятствовать совершению в отношении них правонарушений. Остальные пользователи Интернет, а также те, кто никогда им не пользовался, сходятся во мнении, что преобладать должен государственный контроль (около 62%), который может стать надежным заслоном на пути Интернет-преступности.

Отметим, что органа, координирующего деятельность всех заинтересованных в контроле Интернет и борьбе с Интернет-преступностью в Российской Федерации, не существует. В свою очередь, просто необходимо, чтобы координация всех подразделений, осуществляющих борьбу с Интернет-преступностью, была определена не только на уровне закона, но и на уровне других правовых актов. Также необходим орган, контролирующий развитие законодательства, связанного с функционированием Интернет.

Создание единой структуры, контролирующей деятельность и распространение информации в Интернет, в настоящее время просто необходимо. Ведь кроме борьбы с Интернет-преступностью, которую осуществляют некоторые структуры МВД и ФСБ России, важно устранить такой криминогенный фактор, как распростра-

нение информации, способствующей и содействующей преступлениям, а также идеологически подготавливающей к совершению преступных акций террористической, экстремистской, наркотической, аморальной направленности.

Несмотря на то, что общество требует государственного контроля, необходимо учитывать, что возможности госрегулирования, по мнению специалистов, малоперспективны и весьма дорогостоящи, да к тому же сопряжены еще со значительным ограничением прав и свобод[312], зачастую неприемлемых для государства, провозглашающего демократические принципы. Поэтому в других государствах значительная часть борьбы с Интернет-преступностью возлагается на коммерческие организации. В Китае, например, за размещение противоправной информации несут ответственность, прежде всего, администраторы сайтов и провайдеры (компании, предоставляющие доступ в Интернет), что заставляет их самих следить за информацией, размещенной у них на сайтах[313].

К техническим мерам предупреждения Интернет-преступлений относят различные средства и приспособления, затрудняющие совершение преступлений. Эти меры достаточно подробно изложены в специальной литературе. Существуют различные классификации методов технического противодействия компьютерной и Интернет-преступности.

Например, А. А. Жмыхов делит технические меры предупреждения компьютерной преступности на три вида[314], по отношению к Интернет-преступности эти меры несут более специализированный характер.

Во-первых, *аппаратные*, то есть защищающие непосредственно технические устройства передачи данных от физических воз-

---

[312] Бытко С.Ю. Некоторые проблемы уголовной ответственности за преступления, совершаемые с использованием компьютерных технологий: дис. ... канд. юрид. наук: 12.00.08. — Саратов, 2002. — С. 165.; Алферов О.Л. Право и Интернет в России // Право и информатизация общества. — М., 2002. — С. 125—127.

[313] В США провайдер хотя и не несет уголовной ответственности, но существует множество организаций, консолидирующих компании сферы информационных технологий в вопросах противодействия Интернет-преступности.

[314] Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение: дис. ... канд. юрид. наук: 12.00.08. — М., 2003. — С. 138—139.

действий посторонних сил, например, перехвата сигнала в проводных линиях Интернет, захвата передаваемого беспроводным путем сигнала и т.д. Вопрос безопасности циркуляции сигналов в Интернет-сетях это не только вопрос борьбы с преступностью, но также вопрос национальной безопасности. Перехват сигнала может не только угрожать обороноспособности, но также и политической, и экономической безопасности страны.

Несмотря на то, что перехват с помощью специальных средств при непосредственном контакте не относится к Интернет-преступлениям согласно определению, данному нами в разделе 1.3, правонарушения этого вида зачастую являются подготовкой к Интернет-атаке и, следовательно, профилактика таких преступлений способствует предупреждению уголовно- наказуемых деяний в Глобальной сети.

Практическая реализация данных методов осуществляется с помощью различных технических решений. К ним, например, относятся устройства экранирования аппаратуры и линий связи, средства защиты портов Интернет-устройств и компьютеров, подключенных в Интернет.

Во-вторых, *программные меры* предупреждения предназначены для непосредственной защиты информации и коммуникаций Интернет. Кроме этого с помощью программных средств можно ограничить доступ к той или иной преступной информации, находящейся в Интернет.

Начинать необходимо с программных мер предупреждения преступлений в сфере компьютерной информации (Глава 28 УК РФ), совершаемых посредством Интернет. Данные преступления часто являются необходимым шагом для совершения последующих более сложных преступлений и занимают наибольшую долю в структуре зарегистрированных Интернет-преступлений. Согласно результатам проведенного нами исследования, подавляющее большинство жертв неправомерного доступа это те пользователи Интернет, которые не обеспечены вообще никакими средствами защиты.

Чаще всего неправомерный доступ (ст. 272 УК РФ) осуществлялся непосредственно на компьютеры отдельных пользователей, так как за безопасность канала связи отвечает представитель услуг Интернет (провайдер), в штат которого нанимаются специалисты компьютерных технологий. Защита частными лицами своих

компьютеров таит несколько препятствий. Во-первых, пользователь может иметь средства защиты информации только соответствующие ГОСТам Российской Федерации, и об этом известно злоумышленнику. Например, при шифровании должен использоваться ГОСТ 28147-89 на базе отечественного алгоритма KRYPTON, о недостатках которого имеется немало публикаций на хакерских сайтах.

Во-вторых, большинство использует нелицензионное программное обеспечение, а, следовательно, не может обратиться в службу технической поддержки по вопросам безопасности. Кроме того, нелицензионное программное обеспечение зачастую не поддерживает возможности обновления с целью закрытия основных уязвимостей. В качестве меры предупреждения можно было бы посоветовать частным лицам использовать хотя бы элементарные средства защиты (например, межсетевые экраны), которые спасли бы от 90% попыток неправомерного доступа.

В Интернет всегда можно найти бесплатно распространяемые (freeware) средства защиты, за использование которых не надо платить. К сожалению, не существует эффективных нелицензионных программных и бесплатных средств защиты от такого вида чисто компьютерных преступлений, как *распространение вредоносных программ*. Эффективность так называемых антивирусных программ зависит от количества видов вредоносных программ, с которыми она может бороться. При этом данные о вирусах составлялись годами, поэтому наиболее эффективны давно развивающиеся и постоянно обновляющиеся платные антивирусные.

Кроме преступлений в сфере компьютерной информации посредством Интернет, совершаются другие виды преступлений, многие из которых связаны с распространением той или иной информации (например, ст. 242 УК РФ «Незаконное распространение порнографических материалов или предметов»). При этом в США распространение порнографии посредством Интернет совершенно легально, поэтому закрыть подобный портал не представляется возможным. В свою очередь, можно ограничить доступ к данной информации граждан РФ. Так, в некоторых вузах (например, в ДВГУ) создан запрет на обращение с компьютеров университетской сети к Интернет-сайтам, в адресах которых содержатся компрометирующие ключевые слова, такие как «sex», «porno», что закрывает доступ к большинству порнографических порталов. Также возможна

фильтрация запросов к поисковым службам, чтобы сделать преступную информацию менее доступной.

Представляются перспективными программные системы контроля за содержанием Интернет-форумов и чатов. Так, например, фильтрация высказываний, содержащих ненормативную лексику, затруднила бы совершение таких преступлений, как Клевета (ст. 129 УК РФ), Оскорбление (ст. 130 УК РФ), Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (ст. 282 УК РФ) и т.д.

К комплексным программно-аппаратным средствам можно отнести системы логгирования и отслеживания транзакций посредством Интернет. Зачастую такая деятельность ведется провайдером: кто, во сколько и куда подключился, какая информация, откуда передана. Мониторинг действий, совершаемых в системе, необходим как в профилактической деятельности для нахождения уязвимостей Интернет-системы, так и для расследования уже совершенных Интернет-преступлений. Представляется, что реализация технических мер возможна при соответствующей квалификации специалистов, связанных с компьютерной безопасностью. Как считают некоторые авторы, и с этим нельзя не согласиться, квалификация специалистов по компьютерной и Интернет безопасности по крайней мере не должна уступать квалификации злоумышленников[315].

Экономические меры. Рассматривая проблему профилактики Интернет-преступлений, нельзя не учитывать того факта, что пока экономически не произойдет привлечение компьютерных специалистов из нелегальной сферы деятельности, а также пока останется большой спрос на незаконные услуги Интернет — преступников, серьезных сдвигов в борьбе с сетевой преступностью не предвидится. Ориентированность экономики на добывающую сферу и отсталость информационно-технического сектора создают проблему нехватки рабочих мест для компьютерных специалистов, и это несмотря на недостаток таких специалистов во всех развитых странах.

Развитие отрасли программного и технического компьютерного обеспечения позволило бы России не только избавится от зави-

---

[315] Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. — СПб.: Изд-во «Наука и техника», 2004. — С. 11.

симости от цен на нефть, но и выйти в лидеры мировой экономики. Нашему потенциалу компьютерных специалистов могла бы позавидовать любая развитая страна. Здесь могут сыграть роль государственные меры поддержки бизнеса Информационных технологий в России, в том числе инвестиции в создание новых технологий. Мировой опыт указывает на то, что оптимальному развитию данной сферы помогло предоставление различных налоговых льгот предприятиям и инвесторам, работающим в этом секторе, льготного кредитования за счет средств, заложенных в государственных и региональных программах поддержки предпринимательства.

Также негативно влияет на рост Интернет-преступности высокая цена на программное обеспечение зарубежного производства и, как следствие, на рост так называемого пиратства, т. е. незаконного копирования и продажи программного обеспечения в обход правообладателей (ст. 146 УК РФ). Если бы программное обеспечение продавалось по ценам, устраивающим максимально широкие слои населения, то пиратства как такого не было бы.

Например, Б.Л. Терещенко обращает внимание на то, что существование теневого рынка практически полностью определяется социально-экономической политикой транснациональных монополий, производящих программные продукты. «Если бы компании не были монополистами на рынках интеллектуальной собственности и вели бы более социально ориентированную ценовую политику, ... то многие теневые производства были бы естественным образом втянуты в производство (и распространение) легальной продукции. Они бы выпускали продукцию, цена которой была бы доступна не только для населения высокоразвитых стран, и проблема пиратства уже на государственном уровне (Китай, Болгария, Украина) была бы естественным образом решена»[316]. Представляется, что покупать контрафактную продукцию было бы невыгодно для потребителя.

Именно снижение цен на продукты интеллектуального труда позволит бороться с пиратством в сети Интернет. Кроме этого, пиратство является причиной множества иных преступлений. На-

[316] Терещенко Б.Л. Предупреждение преступлений, посягающих на интеллектуальную собственность. дис. ... канд. юрид. наук: 12.00.08. — М., 2005. — С. 144.

пример, для нелегального использования программный продукт надо сначала взломать, чтобы с ним можно было работать.

Идеологические меры профилактики Интернет-преступности охватывают целый комплекс методов и средств, направленных на устранение в определенных группах и у определенных индивидов антиобщественных установок, а также на выработку негативного общественного отношения к Интернет-преступникам и деяниям, совершаемым хакерами. Идеологическая работа должна быть направлена на определенную аудиторию. Это могут быть широкие общественные слои и представители преступной культуры в Интернет, а также компьютерные специалисты, которые обладают техническим профессионализмом для совершения преступлений в Интернет.

Необходимо отметить, что методы и способы идеологической борьбы в XXI веке сильно отличаются от ранее принятых. Если на широкую общественность еще можно воздействовать через традиционные СМИ (телевидение, газеты, радио), то согласно нашему опросу большинство компьютерных специалистов использует Интернет для чтения новостей (около 64%) и получения деловой информации (около 76%). То есть для этой прослойки общества основной информационной средой, по сравнению со СМИ, является Интернет. Следовательно, с компьютерными специалистами было бы логично вести профилактическую работу посредством сети.

Среди компьютерных специалистов, обучающихся в вузах, высок риск того, что некоторые из них могут быть высококвалифицированными преступниками, и с кем, если не с ними необходимо проводить профилактическую работу. К сожалению, в большинстве вузов Владивостока, готовящих технических специалистов, мало внимания уделяется формированию правового сознания. Так, все правовые дисциплины в них ограничиваются одним семестровым курсом Правоведение, в котором рассматриваются вопросы общего характера, далекие от компьютерных — и Интернет-преступлений. Необходимо выработать единую идеологическую линию, обоснованную научно, в противовес идеологии, созданной в социокультурной среде хакеров. То есть объяснения о недопустимости совершения Интернет-преступлений не должны ограничиваться тем, что это запрещено законом, а иметь под собой серьезную философско-моральную базу. Пропаганда не должна ограничиваться констатацией, что так делать нельзя и это запрещено

законом, а обосновываться в рамках логических доказательств выгодности непреступного пути достижения целей.

Кроме пропагандистских мер, ориентированных на компьютерных специалистов, следует предпринимать меры, направленные на широкую общественность. Так, например, вызывает озабоченность тот факт, что широким слоям населения свойственно идеализировать Интернет-преступника. Идеализация в общественном сознании противоправной деятельности хакеров мешает борьбе с Интернет-преступностью и создает дополнительные стимулы для ведения преступного образа жизни в Глобальной сети. Прежде всего необходимо ограничить поток информации, популяризирующей субкультуру хакеров и создающей необходимые условия для совершения Интернет-преступлений; предоставлять альтернативные сведения об истинном портрете хакера, негативных последствиях его деятельности с тем, чтобы развенчать миф о хакерах как «борцах за свободу», о чистоте помыслов компьютерных преступников.

Это позволило бы обществу контролировать формирование и развитие определенных групп населения, особенно среди подростков и молодежи, склонных к преступному поведению; привело бы к снижению в их среде антиобщественных настроений, взглядов, традиций. Такая профилактика служит инструментом предупреждения конкретных проявлений Интернет-преступности путем поощрения и стимулирования законного образа жизни.

Прогноз по поводу возможностей противодействия субкультуре хакеров достаточно пессимистичен, сегодня это развитое субкультурное объединение, которое охватывает широкие массы людей по всему миру. Продуманность идеологии, удачно сформировавшаяся нравственная система делают субкультуру хакеров легко распространяемой и принимаемой не только людьми, склонными к преступлениям. В свою очередь все антисоциальные и асоциальные молодежные субкультуры образуют устойчивый, адаптирующийся к текущим социальным условиям комплекс, так что противодействие только к данной единичной субкультуре ни к чему не приведет. Представляется, что следует планомерно создавать препятствия распространению и развитию всех асоциальных субкультур.

Правовые меры. Также важным является решение проблемы профилактики и борьбы с Интернет-преступностью на правовом поле. Некоторые авторы считают, что правовые меры предупреж-

дения заключаются в разработке и принятии норм для нейтрализации условий, способствующих совершению конкретных преступлений, стимулирующих к действиям, препятствующим либо пресекающим совершение преступления, а также регламентирующих процесс предупреждения преступлений[317].

По мнению Г. М. Миньковского, правовые меры профилактики содержат: а) совершенствование уголовного, административного, трудового, гражданского, семейного и других отраслей законодательства; б) введение и совершенствование правовых запретов и ограничений, способствующих предупреждению и пресечению возникновения условий для преступлений; в) введение и совершенствование административно-правовых норм, направленных на то, чтобы мерами взыскания за правонарушения пресечь формирование привычек и стереотипов поведения, которые в определенной ситуации могут привести к преступлению (ограничение торговли спиртным и т. д.); г) введение и совершенствование уголовно-правовых норм так называемой двойной превенции, направленных на то, чтобы не допустить тяжких и особо тяжких преступлений путем привлечения к ответственности лиц, создавших благоприятную обстановку для их совершения (ответственность за угрозу убийством, за притоносодержательство и т.д.); д) введение и совершенствование норм, поощряющих пресечение действий преступников и самозащиту от них; е) поощрение добровольного отказа от исполнения готовящегося преступления; ж) поощрение полного раскрытия и выявления преступлений; з) правовую регламентацию деятельности субъектов профилактики; и) воспитание правосознания с тем, чтобы достичь уровня соблюдения правовых норм по личному убеждению; к) воспитание профилактической активности граждан, их готовности помогать в борьбе с преступностью; л) нормативное закрепление стандартов безопасности от преступлений[318].

Мы согласны с тем, что данная классификация наиболее полно раскрывает основные направления предупреждения в области

---

[317] Криминология: Учебник / Под ред. д. ю. н. Бурлакова, д. ю. н. Кропачева. — СПб.: Санкт-Петербургский государственный университет, Питер, 2002. — С. 184.

[318] Криминология: Учебник / Под ред. проф. Н.Ф. Кузнецовой проф., Г.М. Миньковского. — М.: Изд-во БЕК, 1998. — С. 194—195.

Интернет-преступлений. Несмотря на то, что автор рассматривает Интернет-преступность прежде всего с позиции криминологии и уголовного права, активному использованию гражданско-правовых, административно-правовых запретов, формам предупреждения перерастания правонарушений в преступления также должно быть отведено соответствующее место в системе мер профилактики.

Некоторые авторы настаивают на декриминализации некоторых компьютерных преступлений и на их перенесение в КоАП РФ. Например, С.Д. Бражник советует провести межотраслевую дифференциацию ответственности по характеру вреда, вводя ряд норм в КоАП РФ за правонарушения в сфере компьютерной информации[319]. Мы согласны с этой позицией, ведь большинство преступлений, согласно нашим исследованиям, не несёт в себе значительной общественной опасности, наносят минимальный материальный вред и совершаются впервые.

Предлагаем разграничить их по характеру нанесенного материального или морального вреда. В ст. 272 УК РФ необходим признак объективной стороны, заключающийся в доступе, повлекшем уничтожение, блокирование, модификацию и так далее значимой информации. То есть критерием различия между преступлением и административным правонарушением должна стать важность информации. По нашему мнению, следует отделить действительно общественно опасное распространение вредоносных программ для ЭВМ ст. 273 УК РФ от самодублирующихся. Критерием здесь могла бы послужить опасность той или иной распространяемой компьютерной программы.

Метод воздействия на преступность с помощью административных санкций помог бы предупреждению и пресечению условий для возникновения Интернет-преступлений. Например, было бы действенной мерой введение административной ответственности за распространение информации, способствующей совершению Интернет-преступлений, а также средств для совершения Интернет-преступлений, за исключением специализированных порталов и печатных изданий, рассчитанных на специалистов по ком-

[319] Бражник С.Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: дис. ... канд. юрид. наук: 12.00.08. — Ижевск, 2002. — С. 153—154.

пьютерной безопасности. С помощью административного воздействия можно было бы также ограничить распространение информации, призывающей к совершению компьютерных преступлений. Представляется, что не только установление административно-правовых мер может пресечь формирование преступных привычек и антиобщественных наклонностей. Установление ответственности за создание условий для совершения тяжких и особо тяжких преступлений также может содействовать предотвращению деяний, имеющих серьезные социальные последствия.

До сих пор не поднят вопрос об уголовной ответственности за рекламу изготовления, переработки или перевозки наркотических веществ. Примеры в УК РФ есть — так, за рекламирование порнографической продукции предусмотрена уголовная ответственность по ст. 242 УК РФ. Высокую общественную опасность представляют специализированные Интернет-сайты, созданные для потребителей и торговцев наркотиками.

Введение норм УК и КоАП, направленных на борьбу с Интернет-сайтами, пропагандирующими асоциальный и преступный образ жизни, могло бы способствовать решению такой задачи правовой профилактики, как формирование законопослушного правосознания. Представляется, что уменьшение количества пропреступной информации в сети снизило бы число людей, психологически готовых к совершению преступления.

В большинстве случаев при использовании Интернет для совершения преступлений их общественная опасность возрастает. *Во-первых*, преступления могут охватывать неопределенно большой круг потерпевших. *Во-вторых*, использование Интернет создает ощущение безнаказанности в силу удаленности совершаемого деяния от преступника и сложностей в его поиске и пресечении. Представляется, что совершение преступления посредством Интернет отягощает как субъективную, так и объективную составляющие общественной опасности запрещенного уголовным кодексом деяния. Поэтому, на наш взгляд, есть предпосылки для введения в УК РФ нового отягчающего обстоятельства — *совершение преступления посредством компьютерной сети,* с добавлением соответствующих квалифицирующих признаков, тяжесть которых увеличивается при использовании Интернет, других компьютерных сетей (подробней см. § 1.4) и совершение которых посредством компьютерных сетей.

Отсутствие возможности лишать права заниматься определенной деятельностью подразумевает под собой и возможность того, что опасный компьютерный преступник может получить доступ к критически важным коммерческим, государственным и промышленным системам ЭВМ. Представляется, что необходимо ввести дополнительный вид наказания в статьи Главы 28 «Преступления в сфере компьютерной информации»: *лишение права занимать определенные должности или заниматься определенной деятельностью*. Это позволило бы оградить компьютерные системы от лиц, уже совершивших компьютерные преступления. Подобные меры уже давно применяются в США к совершившим компьютерные преступления[320].

С учетом изложенного предлагается добавить в уголовный кодекс в порядке de lege ferenda следующие изменения:

1.) дополнить ч.1 ст. 63 Главы 10 УК РФ пунктом о) следующего содержания:

о) совершение преступления посредством компьютерной сети.

2.) дополнить Главу 25 УК РФ статьей 228^3:

Ст. 228^3. Рекламирование наркотических средств, психотропных веществ или их аналогов

1. Незаконные рекламирование или пропаганда наркотических средств, психотропных веществ или их аналогов, —

наказываются ...

2. Те же деяния, совершенные посредством публикации материалов в *компьютерной сети* или средствах массовой информации, —

наказываются ...

3.) в связи с опасностью того факта, что склонные к компьютерным преступлениям лица могут получить доступ к важным коммерческим и государственным информационным системам внести в статьи 272 и 273 УК РФ следующие изменения с целью запретить широкий доступ к ресурсам ЭВМ и ограничить возможность для повторного совершения преступных деяний в сфере компьютерной информации:

---

[320] Painter C. Supervised release and probation restrictions in hacker cases [Электронный ресурс]/ Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice. — Режим доступа: http://www.cybercrime.gov/usamarch2001_7.htm

ч. 1 ст. 272 УК РФ

наказывается ... *с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до ... лет или без такового*

ч. 2 ст. 272 УК РФ

наказывается ... *с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до ... лет или без такового*

ч. 1 ст. 273 УК РФ

наказываются ... *с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до ... лет или без такового*

ч. 2 ст. 273 УК РФ

наказываются ... *с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до ... лет или без такового*

4.) дополнить Главу 28 УК РФ следующими статьями:

Статья 274[1]. Рассылка компьютерной информации, наносящая ущерб

1. Рассылка компьютерной информации, если это деяние причинило значительный ущерб, —

наказывается ... с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до ... лет или без него.

2. Те же деяния, совершенные группой лиц по предварительному сговору, а также организованной группой, —

наказываются ... с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до ... лет.

Статья 274[2]. Рассылка компьютерной информации вопреки воле получателя

1. Рассылка компьютерной информации вопреки воле получателя, выраженной в конкретном действии, а также непредставление возможности выражения данной воли, —

наказываются ... с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до ... лет или без него.

2. Те же деяния, совершенные неоднократно, либо совершенные группой лиц по предварительному сговору, а также организованной группой, —

наказываются ... с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до ... лет или без него.

Примечание. Условия для выражения своей воли «не получать электронные сообщения» должны быть легко выполнимы материально и физически.

Подводя итог, заметим, что существующие меры борьбы с преступностью в Интернет неэффективны, об этом свидетельствует быстрый рост данной категории правонарушений. Связано это не только с неэффективностью отдельных мер, но прежде всего и с отсутствием целостной системы административных, уголовно-правовых, криминологических мер, направленных на противодействие Интернет-преступности. Только комплекс программ по нейтрализации причин Интернет-преступности и эффективная государственная уголовная политика в этой области способны остановить быстрое развитие этого негативного явления.

Заключение

Современное развитие технологии Интернет и социальных отношений, возникших благодаря ей, характеризуется непрерывным ростом преступлений и других общественно опасных деяний, совершенных посредством всемирной сети, что подтверждено официальной статистикой и научными исследованиями как в России, так и за границей. Учитывая эту глобальную негативную тенденцию в области правовой борьбы с преступностью в Интернет, необходимы решительные меры криминологического и уголовно-правового характера по противодействию и профилактике данного вида преступлений. Принимая во внимание всепроникающее внедрение Интернет во все сферы общественной жизни, представляется, что проблема преступности в Глобальной сети, являясь одной из главных составляющих Информационной безопасности РФ, относится к актуальным, своевременным, имеющим теоретическое и практическое значение.

В настоящее время принципиальное значение приобретают описанные автором в исследовании моменты. Во-первых, сформулировано понятие Интернет-преступления и Интернет-преступности. Проанализированы уголовно-правовые, криминологические признаки и характеристики, исторические аспекты Интернет-преступности и Интернет преступлений.

Отметим, что в работе подробно описан портрет Интернет-преступника и предложена классификация преступников по мотивам и подвидам совершаемых преступлений и т.д. Полученные данные в целом соответствуют ранее проводимым исследованиям в области личности компьютерного и Интернет-преступника, хотя имеется ряд различий. Во-первых, возрастает доля преступников до 18 лет; во-вторых, несмотря на то, что практически во всех преступлениях присутствует корыстный мотив, он зачастую является не единственным и(или) не основным. В-третьих, большинство преступников взяло средства для совершения преступления с так называемых порталов для «хакеров» и, следовательно, знакомо с их субкультурой. В монографии выявлены основные факторы виктимности потерпевших от Интернет-преступлений и предложены меры виктимологической профилактики.

Одним из ключевых моментов монографии является понятие преступной субкультуры хакеров. Реконструирована история

возникновения и развития данной субкультуры, установлены факторы ее влияния на компьютерную и Интернет-преступность. Автор показал соотношение субкультуры хакеров в Интернет с общекриминальной. Исследованы характеристики, идеологические основания, обряды, ритуалы, язык, памятники данной субкультуры. Выявлены основные функции субкультуры «хакеров».

В данной работе проведен анализ общественного мнения разных групп населения в их отношении к проблеме преступности в Интернет. Выявлено, что общество считает государственный контроль информации в Интернет, осуществляемый в настоящее время, недостаточным и требует его ужесточения.

В монографии достаточно подробно исследованы состояние, структура и динамика компьютерной и Интернет-преступности, а также наиболее опасных её подвидов. Проведен анализ криминогенности сети Интернет. Дана правовая и криминологическая оценка общественно опасной деятельности в Интернет, которая не криминализована; выявлена необходимость и достаточные условия для установления уголовной ответственности за нежелательную рассылку электронных сообщений (спам).

Также выявлены детерминанты роста и развития Интернет-преступности. Выделены ее специфические детерминанты. В качестве специфических причин выделены: особые свойства сети Интернет как технического, социального, правого и политического явления; неразвитость сектора информационных технологий в российской экономике; негативное влияние субкультуры хакеров; пробелы и недочеты в российском уголовном и ином законодательстве.

Разработаны меры предупреждения Интернет-преступности организационного, идеологического, технического и правового характера. Среди других шагов по противодействию данному виду общественно опасных деяний необходимо выделить: нейтрализацию негативного влияния субкультуры хакеров, развитие отрасли информационных технологий, модернизацию законодательства РФ в сфере компьютерных технологий.

Современному этапу исследований преступной природы Интернет свойственно постепенное накопление и анализ практической информации. Несмотря на обширное количество специалистов, занимающихся проблемой компьютерной преступности и проблемой компьютерного права, многие вопросы, касающиеся уго-

ловно-правовой и криминологической характеристики Интернет-преступности остаются все еще недостаточно исследованными. Проблема усугубляется сильным отличием Интернет от ранее появлявшихся технологий, что предусматривает рассмотрение данного вопроса в рамках отдельной отрасли Интернет-право, которая не успела до конца сформироваться.

Дальнейшие криминологические исследования должны коснуться, прежде всего, преступной субкультуры в Интернет как среды, наиболее сильно влияющей на облик современной Интернет-преступности. Также необходимо продолжить работу по изучению личности Интернет-преступника, виктимологических аспектов этого вида общественно опасных деяний, выявлению тех или иных негативных условий, содействующих развитию преступности, и разработке эффективных мер противодействия.

Список использованной литературы

Законодательные и другие нормативные акты

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 г. (в ред. от 14.10.2005 г.). — М.: Омега-Л, 2007. — 40 с.

2. Уголовный кодекс Российской Федерации (по состоянию на 20 окт. 2006 г.). — Новосибирск: Сиб. Унив изд-во, 2006. — 192 с.

3. Кодекс Российской Федерации об административных правонарушениях (с изм. и доп. на 10.03.2005 г.). — М.: Эскмо, 2005. — 397 с.

4. Об авторском праве и смежных правах: федеральный закон от 9.07.1993 № 5351-1 (в ред. от 20.07.2004 г.). — М.: Омега-Л, 2005. — 48 с.

5. Об информации, информатизации и защите информации: федеральный закон от 20.02.1995 г. // Новое в законодательстве о защите информации: Сборник документов (Утратил силу). — М.: Омега-Л, 2005. — С. 31 — 42.

6. Об информации, информационных технологиях и о защите информации: федеральный закон от 27.07.2006 № 149-ФЗ. — Новосибирск: Сиб. Унив. Изд-во, 2006. — 16 с.

7. Об участии в международном информационном обмене: федеральный закон от 4.07.1996 г. [Электронный ресурс] // Консультант плюс.

8. О государственной тайне: федеральный закон от 21.07.1993 г. // Новое в законодательстве о защите информации: Сборник документов. — М.: Омега-Л, 2005. — С. 11 — 30.

9. О коммерческой тайне: федеральный закон от 29.07.2004 г. // Новое в законодательстве о защите информации: Сборник документов. — М.: Омега-Л, 2005. — С. 3 — 10.

10. О правовой охране программ для электронных вычислительных машин и баз данных: федеральный закон от 23.09.1992 г. [Электронный ресурс] // Консультант плюс.

11. О рекламе: федеральный закон (по сост. на 15.11.2006 г.). — Новосибирск: Сиб. унив. изд-во, 2006. — 37 с.

12. О связи: федеральный закон от 07.07.2003 г. [Электронный ресурс] // Консультант плюс.

13. О средствах массовой информации: федеральный закон от 27.12.1991 г. — М.: АСТ 2000, 2000. — 43 с.

Законодательство зарубежных стран

14. Окинавская хартия глобального информационного сообщества [Электронный ресурс] // Законодательство в сфере Интернета. — Режим доступа: http://www.internet-law.ru/intlaw/laws/okinava.htm

15. Уголовный кодекс Китайской Народной Республики / Под ред. и с предисл. проф. А.И. Коробеева; Пер. с кит. — Владивосток: Изд-во Дальневосточного ун-та, 1999. — 176 с.

16. Australia, Crimes Act 1914, Part VIA [Электронный ресурс] // Scaleplus. — Режим доступа: http:// scaleplus.law.gov.au

17. SPAM ACT 2003 [Электронный ресурс] // The Attorney General's department. — Режим доступа: http://scaleplus.law.gov.au/html/pasteact/3/3628/top.htm

18. Terrorism Act 2000 [Электронный ресурс] // Office of public sector information. — Режим доступа: http://www.opsi.gov.uk/Acts/acts2000/20000011.htm

19. US Code [Электронный ресурс]/ Legal Infomation Institute & Cornell Law School. — Режим доступа: http://www4. law.cornell.edu/uscode/

Книги, монографии, сборники, статьи

20. Алферов О.Л. Право и Интернет в России // Право и информатизация общества. — М., 2002. — С. 124—129.

21. Бабаев М.М. Лекция по теме: феномены молодежной преступности // Российский криминологический взгляд. — 2007. — № 2. — С. 106—116.

22. Бабаев М.М. Социально-психологические компоненты детерминации преступного поведения молодежи // Российский криминологический взгляд. — 2005. — № 1. — С. 65—72.

23. Батурин Ю.М., Жодзишкий А.М. Компьютерная преступность и компьютерная безопасность. — М. : Изд-во юрид. лит., 1991. — 160 с.

24. Быков В. Совершенствование уголовной ответственности за преступления, сопряженные с компьютерными технологиями / В. Быков, А. Нехорошев, В. Черкасов // Уголовное право. — 2003. — № 3. — С. 9—11.

25. Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия / В. Б. Вехов ; под. ред. акад. Б.П. Смагоринского. — М. : Право и закон, 1996. — 182 с.

26. Вехов В.Б. Правовые и криминалистические аспекты понятия компьютерная информация // "Черные дыры" в российском законодательстве. — 2004. — № 3. — С. 234 — 245.

27. Вехов В.Б. Проблемы определения понятия компьютерной информации в свете унификации уголовных законодательств стран СНГ // Уголовное право. — 2004. — № 4. — С. 15 — 17.

28. Войниканис Е.А. Информация. Собственность. Интернет: традиция и новеллы в современном праве / Е.А. Войниканис, М.В. Якушев. — М. : Волтерс Клувер, 2004. — 176 с.

29. Волеводз А.Г. Следы преступлений, совершенных в компьютерных сетях // Российский следователь. — 2002. — № 1. — С. 4 — 12.

30. Гаврилов М.В. Извлечение и исследование компьютерной информации / М.В. Гаврилов, А.Н. Иванов // Уголовное право. — 2004. — № 4. — С. 74 — 76.

31. Гиряева В.Н. Интернет и молодежь: правовые аспекты // Право и информатизация общества. — М., 2002. — С. 165 — 172.

32. Гончаров Д. Квалификация хищений, совершаемых с помощью компьютеров // Законность. — 2001. — № 11. — С. 31 — 33.

33. Горшенков Г.Н. Киберкриминология: к понятию «информаионная преступность» // Российский криминологический взгляд. — 2005. — № 4. — С. 93 — 96.

34. Гузеева О. Склонение или пропаганда? // Законность. — 2008. — № 3. — С. 35 — 37.

35. Данильян О.Г. Философия права: Учебник / О.Г Данильян, Л.Д. Байрачная, С.И. Максимов и др. / под. ред. О.Г. Данильяна. — М. : Изд-во Эксмо, 2006. — 416 с.

36. Долгова А.И. Преступность в России начала XXI века и реагирование на нее / А.И. Долгова и коллектив авторов ; под ред. профессора А.И. Долговой. — М. : Российская криминологическая ассоциация, 2004. — 124 с.

37. Дремлюга Р.И. Виктимологические аспекты Интернет-преступности // Право и современность: проблемы и пути решения. Материалы конференции молодых ученых, аспирантов и студентов. — Владивосток : Изд-во Дальневост. ун-та, 2006. — С. 92 — 96.

38. Дремлюга Р.И. Виктимология неправомерного доступа к компьютерной информации посредством Интернет // Вестник Южно-Сахалинского филиала ДВЮИ МВД России. № 1 (3). — Южно-Сахалинск, 2006. — С. 12 — 15.

39. Дремлюга Р.И. Интернет-преступность: криминологическое исследование общественного мнения // Культурно-экономическое сотрудничество стран Северо-Восточной Азии: Материалы Второго международного симпозиума, 18 — 19 мая 2006 г.: в 2 т. / под. ред. Ю.М. Сердюкова. Т. 1. — Хабаровск: Изд-во ДВГУПС, 2006. — С. 181 — 188.

40. Дремлюга Р.И. Интернет-преступность как угроза экономической безопасности / Р.И. Дремлюга, Н.А. Крайнова, И.Г. Сергеева // Социально-экономические проблемы развития России и проблемы глобализации и проблемы глобализации: потенциал возможного: Сборник научных статей ; под общ. ред. В.В. Тумалева. — СПб.: Изд-во Политехн. ун-та, 2007. — С. 181 — 184.

41. Дремлюга Р.И. Криминологические аспекты террористической деятельности в Интернет // Современная юридическая наука и практика. Проблемы и перспективы: Материалы научно-практической конференции. — Владивосток : Изд-во Дальневост. ун-та, 2007. — С. 145 — 151.

42. Дремлюга Р.И. Криминологическая характеристика личности преступника // Уголовно-правовые и криминологические проблемы борьбы с преступностью: сб. научн. тр. / под ред. А.Л. Репецкой. — Вып. 3. — Иркутск : Изд-во БГУЭП, 2006. — С. 106 — 114.

43. Дремлюга Р.И. Криминологическое значение субкультуры хакеров // Ученые записки юридического факультета / под ред. А.А. Ливеровского. — СПб. : Изд-во С.-Петерб. ун-та экономики и финансов, 2007. — Вып. 7 (17). — С. 11 — 15.

44. Дремлюга Р.И. Наркопреступность в Интернет // Интеллектуальный потенциал вузов — на развитие дальневосточного региона России: материалы VII Международной конференции студентов, аспирантов и молодых ученых. В 8 кн.: Кн. 7 / Институт права. — Владивосток : Изд-во ВГУЭС, 2005. — С. 58 — 61.

45. Дремлюга Р.И. Распространение порнографии в Интернет // Стратегии и тенденции развития Российского права и законодательства в XXI веке: Материалы конференции преподавателей, аспирантов и студентов 3 апреля 2007 г. — Владивосток : Изд-во Дальневост. ун-та, 2007. — С. 31 — 36.

46. Дремлюга Р.И. Рассылка электронной почты и проблемы уголовной ответственности // Уголовное право: стратегия развития в XXI веке: сб. материалов третьей Международной научно-практической конференции. — М., 2006. — С. 225 — 228.

47. Дремлюга Р.И. Субкультурный фактор, как причина компьютерной преступности // Дальневосточный криминалистические чтения: Сб. науч. тр. / Отв. ред. В.В. Яровенко. — Владивосток: Изд-во Дальневост. ун-та, 2005. — С. 80—83.

48. Завидов Б. Сфера высоких технологий как объект преступления // Уголовное право. — № 3. — 2002. — С. 109—112.

49. Заянчуковский С.О. Противодействие распространению спама: украинский опыт криминализации // Уголовное право: стратегия развития в XXI веке: материалы 4-й Международной научно практической конференции. — М.: ТК Велби, Изд-во «Проспект», 2007. — С. 622—623.

50. Илюшин Д.А. Возбуждение дел по «сетевым» преступлениям // Российская юстиция. — 2007. — № 2. — С. 55—57.

51. Касперский Е. В. Компьютерные вирусы: что это такое и как с ними бороться. — М.: СК Пресс, 1998. — 288 с.

52. Касперски К. Компьютерные вирусы изнутри и снаружи. — СПб.: Питер, 2007. — 527 с.

53. Касперски К. Техника и философия хакерских атак — записки мыщ'а. — М.: СОЛОН-Пресс, 2004. — 272 с.

54. Касперски К. Техника отладки программ без исходных текстов / К. Касперски. — СПб.: БХВ-Петербург, 2005. — 820 с.

55. Кашапов Р.М. Проблемы с распространением детской порнографии в глобальной сети Интернет / Р.М. Кашапов, С.С. Наумов // Вестник Дальневосточного юридического института МВД России. — 2004. — № 2. — С.72—79.

56. Кочетков А. Меры противодействия криминальной идеологии в культуре // Законность. — 2002. — № 4. — С. 51—52.

57. Колмыков В.В. Криминологическая характеристика компьютерных преступлений // Вестник Дальневосточного юридического института МВД России. — 2005. — № 1(8) — С. 84—87.

58. Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. В. М. Лебедев. — 5-е изд., доп. и испр. — М.: Юрайт-Издат, 2006. — 921 с.

59. Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. А.А. Чекалин; Под ред. В.Т. Томина, В.С. Устинова, В.В. Сверчкова. — 2-е изд., исп. и доп. — М.: Юрайт-Издат, 2004. — 1038 с.

60. Комментарий к Уголовному кодексу Российской Федерации с постатейными материалами и судебной практикой / Под общ. ред. С.И. Никулина. — М.: Изд-во «Менеджер»; Изд-во «Юрайт», 2001. — 1184 с.

61. Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. В.И. Радченко; Науч. ред. А.С. Михлин. — М.: Спарк, 2000. — 862 с.

62. Комментарий к Уголовному кодексу Российской Федерации. Расширенный уголовно-правовой анализ / Под общ. ред. В.В. Мозякова. — М.: Экзамен. — 864 с.

63. Корнилс К. Локализация места ответственности за преступления, связанные с Интернетом // Право и информатизация общества. — М., 2002. — С. 298 — 302.

64. Коробеев А.И. Уголовно-правовая политика: тенденции и перспективы / А.И. Коробеев, А.В. Усс, Ю.В. Голик. — Красноярск: Изд-во Красноярского университета, 1991. — 240 с.

65. Криминология: учеб. для студентов вузов / А.И. Гуров и др. / Под. науч. ред. Н.Ф. Кузнецовой, В.В. Лунеева. — М.: Волтерс Клувер, 2005. — 640 с.

66. Криминология / Под. ред. Дж. Ф. Шели / Пер. с англ. — СПб.: Питер, 2003. — 864 с.

67. Криминология: Учебник для вузов / Под общ. ред. д.ю.н. проф. А.И. Долговой. — 2-е изд., перераб. и доп. — М.: Изд-во НОРМА, 2003. — 848 с.

68. Криминология: Учебник для вузов / Под общ. ред. д.ю.н. проф. А.И. Долговой. — 3-е изд. перераб. и доп.— М.: Норма, 2005. — 912 с.

69. Криминология: Учебник / под. ред. В.Н. Бурлакова, Н.М. Кропачева. — СПб.: Санкт-Петербургский гос. ун-т., 2002. — 432 с.

70. Кудрявцев В.Н. Причинность в криминологии (О структуре преступного поведения), М: Изд-во Юридическая литература, 1968. — 176 с.

71. Кураков Л.П. Информация как объект правовой защиты / Л.П. Кураков, С.Н. Смирнов. — М.: Гелиос, 1998. — 240 с.

72. Левикова С.И. Молодежная субкультура. — М., 2004. — 608 с.

73. Левин М. Как стать хакером: Интеллектуальное руководство по хакингу и фрикингу. — 3-е изд. — М.: ЗАО «Новый издательский дом», 2005. — 320 с.

74. Ломакин П. Антихакинг / П. Ломакин, Д. Шрейн. — М.: Майор, 2002. — 510 с.

75. Лопатина Т.М. Виктимологическая профилактика компьютерных преступлений // Российская юстиция. — 2006. — № 4. — С. 51 — 54.

76. Лопатина Т.М. Противодействие преступлениям в сфере компьютерной информации // Законность. — 2006. — № 6. — С. 50—51.

77. Луцкер А.П. Авторское право в цифровых технологиях и СМИ: с научными комментариями к.ю.н. А.Г. Серго — М.: КУДИЦ-ОБРАЗ, 2005. — 416 с.

78. Ляпунов Ю. Ответственность за компьютерные преступления / Ю. Ляпунов, В. Максимов // Законность. — 1997. — № 1. — С. 8—15.

79. Мазуров В.А. Компьютерные преступления: классификация и способы противодействия. — М.: «Палеонтип», 2002. — 148 с.

80. Менжега М.М. Особенности установления личности хакера // Закон и право. — 2004. — № 8. — С. 62—64.

81. Меркурьев А.В. Социолого-криминологические аспекты борьбы с преступлениями в сфере компьютерной информации / А.В. Меркурьев, С.С. Наумов // Вестник Дальневосточного юридического института МВД России. — 2002. — № 2(3) — С. 69—76.

82. Мирзоев Б.Г. Киберпреступность: угрозы безопасности информационного общества // Современное право. — 2006. — № 1. — С. 13—18.

83. Михайленко Е.В. Информационное право в свете развития глобальной сети Интернет // Закон и право. — 2004. — № 8. — С. 60—62.

84. Нерсесянц В.С. Философия права: Учебник для вузов. — М.: Изд-во НОРМА, 2004. — 656 с.

85. Новак Д. Обнаружение нарушений безопасности в сетях : Пер. с англ / Д. Новак, С. Норткат. — 3-е издание. — М.: Издат. дом «Вильямс», 2003. — 448 с.

86. Номоконов В.А. Актуальные проблемы борьбы с киберпреступностью // Інформаційні технології та безпека. — Киев, 2003. — С. 101—107.

87. Номоконов В.А. Глобализация информационных процессов и преступность // Інформаційні технології та безпека. — Киев, 2002. — С. 95—103.

88. Овчинников Б.Д. Вопросы теории криминологии. — СПб.: Изд-во Ленинградского ун-та, 1982. — 78 с.

89. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография. — М.: Норма, 2004. — 432 с.

90. Осипенко А.Л. Уголовно-правовые и иные средства противодействия обороту материалов с порнографическими изображениями несовершеннолетних в сети Интернет // Уголовное право. — 2007. — № 1. — С. 110 — 114.

91. Проблемы причинности в криминологии и уголовном праве: Межвузовский тематический сборник. — Владивосток: Изд-во Дальневост. ун-та, 1983. — 144 с.

92. Разуваев В.Э. Правовые вопросы борьбы со спамом как средством ведения информационной войны // Государство и право. — 2006. — № 7. — С. 83 — 89.

93. Расследование неправомерного доступа к компьютерной информации: учебное пособие / Под. Ред. д.ю.н. проф. Н.Г. Шурухнова. — Изд. 2-е, перераб. и доп. — М.: Московский университет МВД России, 2004. — 352 с.

94. Рассолов И.М. Право и Интернет. Теоретические проблемы / И.М. Рассолов. — М.: Изд-во НОРМА, 2003. — 336 с.

95. Репецкая А.Л. Российский криминальный рынок услуг: структура и характеристика отдельных видов // Криминологический журнал Байкальского университета экономики и права. — 2008. — № 1. — С. 24 — 33.

96. Российское уголовное право. Курс лекций. Т.1. Преступление / Под ред. проф. А.И. Коробеева. — Владивосток: Изд-во Дальневост. ун-та, 1999. — 604 с.

97. Российское уголовное право: Курс лекций. Т. 5. Преступления против общественной безопасности и общественного порядка / Под ред. проф. А.И. Коробеева. — Владивосток: Изд-во Дальневост. ун-та, 1999. — 592 с.

98. Рохлин В. Проблемы уголовного преследования за киберпреступления (детская порнография в Интернете) / В. Рохлин, С. Кушниренко // Законность. — № 3. — 2007. — С. 28 — 31.

99. Середа С.А. Сложности толкования терминов «вредоносная программа» и «неправомерный доступ» / С.А. Середа, Н.Н. Федотов // Российская юстиция. — № 2. — 2007. — С. 58 — 61.

100. Старостина Е.В. Защита от компьютерных преступлений и кибертерроризма / Е.В Старостина, Д.Б. Фролов. — М.: Эксмо, 2005. — 192 с.

101. Степанов-Егиянц В.Г. Ответственность за компьютерные преступления // Законность. — № 12. — 2005. — С. 49 — 51.

102. Тедеев А.А. Информационное право (право Интернета): Учебное пособие. — М.: Эксмо, 2005. — 304 с.

103. Трайнин А.П. Состав преступления по советскому уголовному праву. — М.: Госюриздат, 1951. — 387 с.

104. Трунцевский Ю. Общая характеристика составов преступлений, сопряженных со ст. 146 УК РФ в аудиовизуальной сфере // Уголовное право. — 2003. — № 1. — С. 48 — 49.

105. Уголовное право. Общая часть. Учебник / Под ред. проф. Л.Д. Гаухмана и проф. С.В. Максимова. — М.: Эксмо, 2004. — 416 с.

106. Уголовное право Российской Федерации. Общая часть: Учебник для вузов / Под ред. А.И. Рарога, А.С. Самойлова. — М.: Высшее образование, 2005. — 495 с.

107. Уголовное право. Особенная часть. Учебник / Под ред. проф. Л.Д. Гаухмана и проф. С.В. Максимова. — М.: Эксмо, 2005. — 704 с.

108. Уорли Б. Интернет: реальные и мнимые угрозы / Пер. с англ. — М.: КУДИЦ-ОБРАЗ, 2004. — 320 с.

109. Хатч Б. Секреты хакеров. Безопасность Linux: Пер с англ. / Б. Хатч, Д. Ли, Д. Курц. — М.: Издательский дом «Вильямс», 2004. — 704 с.

110. Форд Дж. Ли Персональная защита от хакеров. Руководство для начинающих / Пер. с англ. — М.: КУДИЦ-ОБРАЗ, 2002. — 270 с.

111. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. — СПб.: Наука и техника, 2004. — 384 с.

112. Шестаков Д.А. Преступность как свойство общества. — СПб.: Лань, 2001. — 259 с.

113. Шнайдер Г.Й. Криминология: Пер. с нем. / Под общ. ред. с предисл. Л.О. Иванова. — М.: Издательская группа «Прогресс»-«Универс», 1994. — 504 с.

114. Ястребов Д.А. Институт уголовной ответственности в сфере компьютерной информации (опыт международно-правового сравнительного анализа) // Государство и право. — 2005. — № 1. — С. 53 — 63.

Книги, монографии, сборники, статьи на иностранных языках

115. Bidwell T. Hack proofing your identity in the information age. — Syngress Publishing. Inc.,2002. — ISBN: 1931836515. — 370 p.

116. Chirillo J. Hack Attacks Revealed. — New York:Wiley Computer Publishing, 2001. — 944 p.

117. Cornwall H. The hackers handbook. — E.A. Brown Co., 1986. — 168 p.

118. Mungo P. The Extraordinary underworld of Hackers, Phreakers, Virus writers, and Keyboard criminals / P. Mungo, B. Clough. — New york: Random house, 1992. — 243 p.

119. Schweitzer D. Incident response: computer forensics toolkit. Wiley, 2003. — ISBN: 0764526367. — 360 p.

120. Shinder D.L. Scene of the cibercrime: computer forensics handbook. — Syngress Publishing. Inc., 2003. — 752 p.

121. Sinrod E.J., Reilly W.P. Cyber-Crimes: A practical approach to the application of federal computer crime laws // Santa Clara computer and high technology law journal. — Vol. 16. — №2. — P. 2—53.

Диссертации и авторефераты диссертаций

122. Айсанов Р.М. Состав неправомерного доступа к компьютерной информации в российском, международном и зарубежном уголовном законодательстве: дис. ... канд. юрид. наук: 12.00.08. — М., 2006. — 191 с.

123. Алоян А.А. Предупреждение распространения субкультуры наркомании в молодежной среде: дис. ... канд. юрид. наук: 12.00.08. — М., 2002. — 174 с.

124. Барсукова С.Ю. Неформальная экономика: структура и функциональная специфика элементов: дис. ... докт. соц. наук: 22.00.03. — М., 2004. — 331 с.

125. Бражник С.Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: дис. ... канд. юрид. наук: 12.00.08. — Ижевск, 2002. — 189 с.

126. Булгакова О.А. Уголовная ответственность за незаконное распространение порнографических материалов или предметов: : дис. ... канд. юрид. наук: 12.00.08. — Ставрополь, 2003. — 178 с.

127. Бытко С.Ю. Некоторые проблемы уголовной ответственности за преступления, совершаемые с использованием компьютерных технологий: дис. ... канд. юрид. наук: 12.00.08. — Саратов, 2002. — 204 с.

128. Воробьев В.В. Преступления в сфере компьютерной информации (юридическая характеристика и квалификация): дис. ... канд. юрид. наук: 12.00.08. — Нижний Новгород, 2000. — 201 с.

129. Гаджиев М.С. Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики

Дагестан): дис. ... канд. юрид. наук: 12.00.08. — Махачкала, 2004. — 168 с.

130. Геллер А.В. Уголовно-правовые и криминологические аспекты обеспечения защиты электронной информации и Интернета: дис. ... канд. юрид. наук: 12.00.08. — М., 2006. — 219 с.

131. Демидов Р.С. Теневая экономика криминологический анализ: дис. ... канд. юрид. наук: 12.00.08. — М., 2002. — 191с.

132. Денисенко М.В. Уголовная ответственность за незаконное распространение порнографических материалов или предметов: : дис. ... канд. юрид. наук: 12.00.08. — М., 2004. — 182 с.

133. Денисов Н.Л. Влияние криминальной субкультуры на становление личности несовершеннолетнего преступника: дис. ... канд. юрид. наук: 12.00.08. — М., 2002. — 194 с.

134. Добровольский Д.В. Актуальные проблемы борьбы с компьютерной преступностью: дис. ... канд. юрид. наук: 12.00.08. — М., 2005. — 218 с.

135. Доронин А.М. Уголовная ответственность за неправомерный доступ к компьютерной информации: дис. ... канд. юрид. наук: 12.00.08. — М., 2003. — 154 с.

136. Дубягина О.П. Криминологическая характеристика норм обычаев и средств коммуникации криминальной среды: автореферат на соискание степени ... канд. юрид. наук: 12.00.08. — М., 2008. — 26 с.

137. Евдокимов К.Н. Уголовно-правовые и криминологические аспекты противодействия неправомерному доступу к компьютерной информации: дис. ... канд. юрид. наук: 12.00.08. — Иркутск, 2006. — 198 с.

138. Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение: дис. ... канд. юрид. наук: 12.00.08. — М., 2003. — 178 с.

139. Зыков Д.А. Виктимологические аспекты предупреждения компьютерного мошенничества: дис. ... канд. юрид. наук: 12.00.08. — Владимир, 2002. — 211 с.

140. Ильина Н.В. Особенности причинного комплекса преступности в условиях перехода к рыночной экономике: дис. ... канд. юрид. наук: 12.00.08. — М., 1998. — 214 с.

141. Казарян Э.А. Совершенствование правового регулирования распространения информации в Интернете: дис. ... канд. юрид. наук: 12.00.14. — М., 2004. — 213 с.

142. Кесареева Т.П. Криминологическая характеристика и предупреждение преступности в Российском сегменте сети Интернет: дис. ... канд. юрид. наук: 12.00.08. — М., 2002. — 195 с.

143. Красненкова Е.В. Обеспечение информационной безопасности в Российской Федерации уголовно-правовыми средствами: дис. ... канд. юрид. наук: 12.00.08. — М., 2006. — 188 с.

144. Крашенинников Д.А. Последствия экологических преступлений (понятие, виды, общая характеристика): дис. ... канд. юрид. наук: 12.00.08. — Казань, 2007. — 26 с.

145. Кротов С.Е. Дифференциация уголовной ответственности в зависимости от категоризации преступлений, квалифицирующих признаков и обстоятельств, отягчающих наказание: дис. ... канд. юрид. наук: 12.00.08. — М., 2005. — 176 с.

146. Куликов Е.М. Незаконная банковская деятельность: уголовно-правовые и криминологические проблемы: дис. ... канд. юрид. наук: 12.00.08. — Ставрополь, 2001. — 178 с.

147. Лазарева И.В. Расследование преступлений, связанных с несанкционированным доступом к сети сотовой радиотелефонной связи: автореферат на соискание степени ... канд. юрид. наук: 12.00.09. — Иркутск, 2007. — 23 с.

148. Лебедева Н.Н. Правовая культура личности и Интернет (Теоретический аспект): дис. ... канд. юрид. наук: 12.00.01. — М., 2004. — 211 с.

149. Лунев А.А. Терроризм как объект криминологического изучения: дис. ... канд. юрид. наук: 12.00.08. — Ростов-на-дону, 2004. — 180 с.

150. Малыковцев М.М. Уголовная ответственность за использование и распространение вредоносных программ для ЭВМ: дис. ... канд. юрид. наук: 12.00.08. — М., 2006. — 186 с.

151. Менжега М.М. Криминалистические проблемы расследования создания, использования и распространения вредоносных программ для ЭВМ: дис. ... канд. юрид. наук: 12.00.09. — Саратов, 2005. — 238 с.

152. Молчанов С.В. Административно-правовые основания ограничения конституционного права человека на распространение информации через Интернет в Российской Федерации: дис. ... канд. юрид. наук: 12.00.14. — М., 2005. — 193 с.

153. Павлова А.А. Субкультура теневой экономической деятельности: сущность и факторы воспроизводства в России: дис. ... канд. соц. наук: 22.00.03. — М., 2004. — 158 с.

154. Петросян О.Ш. Уголовная ответственность за изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних: дис. ... канд. юрид. наук: 12.00.08. — М., 2005. — 187 с.

155. Рябцев Р. А. Современная правовая реформа в России и правосознание: дис. ... канд. юрид. наук: 12.00.01. — Ростов-на-дону, 2005. — 173 с.

156. Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: дис. ... канд. юрид. наук: 12.00.08. — М., 1998. — 161 с.

157. Соловьев Л.Н. Расследование преступлений, связанных с созданием, использованием и распространением вредоносных программ для ЭВМ: дис. ... канд. юрид. наук: 12.00.09. — М., 2003. — 275 с.

158. Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики: дис. ... канд. юрид. наук: 12.00.08. — Иркутск, 2006. — 237 с.

159. Степанов-Егиянц В.Г. Преступления в сфере безопасности обращения компьютерной информации: сравнительный анализ: дис. ... канд. юрид. наук: 12.00.08. — М., 2005. — 168 с.

160. Терещенко Б.Л. Предупреждение преступлений, посягающих на интеллектуальную собственность: дис. ... канд. юрид. наук: 12.00.08. — М., 2005. — 217 с.

161. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук: 12.00.08. — Владивосток, 2005. — 235 с.

162. Тулегенов В.В. Криминальная субкультура и ее криминологическое значение: дис. ... канд. юрид. наук: 12.00.08. — Ростов-на-Дону, 2003. — 228 с.

163. Ушаков С.И. Преступления в сфере обращения компьютерной информации (Теория, законодательство, практика): дис. ... канд. юрид. наук: 12.00.08. — Ростов-на-дону, 2000. — 176 с.

164. Числин В.П. Уголовно-правовые меры защиты информации от неправомерного доступа: дис. ... канд. юрид. наук: 12.00.08. — М., 2004. — 134 с.

165. Шаповалова Г.М., Возможность использования информационных следов в криминалистике: автореферат на соискание степени ... канд. юрид. наук: 12.00.09. — Владивосток, 2006. — 23 с.

166. Шарков А.Е. Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации: дис. ... канд. юрид. наук: 12.00.08. — Ставрополь, 2004. — 174 с.

167. Ястребов Д.А. Неправомерный доступ к компьютерной информации: уголовно-правовые и криминологические аспекты: дис. ... канд. юрид. наук: 12.00.08. — М., 2005. — 243 с.

Электронные ресурсы на русском языке

168. Богдановская И.Ю. Законодательство о спаме: зарубежный опыт и российские перспективы [Электронный ресурс] / И.Ю.Богдановская, Е.К. Волчинская // Информационное право. — Режим доступа: http://www.infolaw.ru/lib/2005-1-spam # 15

169. Вершинин М. Современные молодежные субкультуры: хакеры [Электронный ресурс] // Сайт практической психологии ПСИ-ФАКТОР. — Режим доступа: http://www.psyfactor.org/lib/vershinin4.htm

170. Голубев В.А. Доходы от детского порнобизнеса превышают доходы колумбийской наркомафии [Электронный ресурс] / Центр исследования компьютерной преступности. — Режим доступа: http://www.crime-research.ru/analytics/gol100207/

171. Голубев В.А. Киберпреступность — угрозы и прогнозы [Электронный ресурс] / Центр исследования компьютерной преступности. — Режим доступа: http://www.crime-research.ru/articles/golubev_071

172. Голубев В.А. Компьютерная преступность — проблемы борьбы с Интернет-педофилией и детской порнографией [Электронный ресурс] / Центр исследования компьютерной преступности. — Режим доступа: http://www.crime-research.ru/articles/golubev2106

173. Лукацкий А. Хакеры управляют реактором [Электронный ресурс] / Центр исследования компьютерной преступности. — Режим доступа: http://www.crime-research.org/library/Lukac0103.html

174. Сухаренко А.Н. Распространение детской порнографии через сеть Интернет [Электронный ресурс] / Владивостокский центр исследования организованной преступности. — Режим доступа: http://www.crime.vl.ru/index.php?p=1077&more=1&c=1&tb=1&pb=1#more1077

175. Шевченко С. Профессия — хакер (часть II) [Электронный ресурс] / Центр исследования компьютерной преступности. — Режим доступа: http://www.crime-research.ru/analytics/hacker12/

Электронные ресурсы на иностранных языках

176. CERT/CC Statistics 1988-2006[Электронный ресурс] / CERT. — Режим доступа: http://www.cert.org/stats/cert_stats.html

177. Conway M. Terrorist "use" of the Internet and Fighting back. [Электронный ресурс] / Oxford Internet Institute University of oxford. — Режим доступа: http://www.oii.ox.ac.uk/research/cybersafety/extensions/pdfs/papers/maura_conway.pdf

178. Gang F. Piracy in China [Электронный ресурс] / Project Syndicate. — Режим доступа: http://www.project-syndicate.org/commentary/fang8

179. It's Not Just Fun and «War Games» - Juveniles and Computer Crime [Электронный ресурс]/ Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice. — Режим доступа: http://www.cybercrime.gov/usamay2001_7.htm

180. Kazakhstan Hacker Sentenced to Four Years Prison for Breaking into Bloomberg Systems and Attempting Extortion [Электронный ресурс] / Computer Crime & Intellectual Property Section U.S. Department of Justice. — Режим доступа: http://www.cybercrime.gov/zezevSent.htm

181. Kevin Mitnick sentenced to nearly four years in prison [Электронный ресурс] / Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice. — Режим доступа: http://www.cybercrime.gov/mitnick.htm

182. Lemos R. Cyberterrorism: The real risk [Электронный ресурс] / Центр исследования компьютерной преступности. — Режим доступа: http://www.crime-research.org/library/Robert1.htm

183. Orange County Computer Hacker Sentenced to Prison for Breaking into University Computers, NASA Systems [Электронный ресурс] / Computer Crime & Intellectual Property Section U.S. Department of Justice. — Режим доступа: http://www.cybercrime. gov/diekmanSent.htm

184. Painter C. Supervised release and probation restrictions in hacker cases [Электронный ресурс] / Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice. — Режим доступа: http://www.cybercrime.gov/usamarch2001_7.htm

185. Salgado, Richard P. Working with Victims of Computer Network Hacks [Электронный ресурс] / Computer Crime and

Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice. — Режим доступа: http://www.cybercrime.gov/usamarch2001_6.htm

186. Shimeall T. Countering cyber war [Электронный ресурс]/ T. Shimeall, P. Williams, C. Dunlevy // NATO Review vol. 49. — 2001. — №4 (Winter). — Режим доступа: http://www.nato.int/docu/review/2001/0104-04.htm

187. The electronic frontier: The challenge of unlawful conduct involving the use of the Internet: A Report of the President's Working Group on Unlawful Conduct on the Internet [Электронный ресурс] / Департамент Юстиций США. — Режим доступа: http://www.usdoj.gov/criminal/cybercrime/unlawful.htm

188. Xiao Qiang. Cniha's Virtual Revolution [Электронный ресурс] / Project Syndicate. — Режим доступа: http://www.project-syndicate.org/commentaries/commentary_text.php4?

Научное издание

Дремлюга Роман Игоревич

ИНТЕРНЕТ-ПРЕСТУПНОСТЬ

Монография

Редактор *В.Г. Дроздов*
Дизайн обложки *С.В. Филатова*
Компьютерная верстка *С.А. Стогний*

Подписано в печать 21.05.2008.
Формат 60x84/16. Усл. печ. л. 13,95. Уч.-изд. л. 14,51.
Тираж 300 экз. Заказ

Издательство Дальневосточного университета
690950, Владивосток, ул. Октябрьская, 27.

Отпечатано в типографии
Издательско-полиграфического комплекса ДВГУ.
690950, Владивосток, ул. Алеутская, 56.