МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «ОРЛОВСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Е.А. Маслакова

НЕЗАКОННЫЙ ОБОРОТ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ: УГОЛОВНО-ПРАВОВЫЕ И КРИМИНОЛОГИЧЕСКИЕ ПРОБЛЕМЫ

Монография

Орел
ОрЮИ МВД России
2012

УДК34С5
ББК 67.99(2)8
М31

Рецензенты:

- Козлов Г. Т., кандидат юридических наук, доцент
(ФГБОУ ВПО «Государственный университет – УНПК»);
- Минаков Г. Л., кандидат юридических наук, доцент
(ФГБОУ ВПО «Российская академия народного хозяйства и государственной службы при Президенте РФ», Орловский филиал).

Ì àñëàêîâà Å.À.

М31 **Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические проблемы**: монография / Е.А. Маслакова. – Орёл: ОрЮИ МВД России, 2012. – 111 с.

Монография посвящена исследованию уголовно-правовых и криминологических особенностей одного из видов компьютерных преступлений, связанного с созданием, использованием и распространением вредоносных компьютерных программ. В ней раскрываются криминообразующие и квалифицирующие признаки таких преступлений, рассматриваются особенности преступности данного вида, ее криминологические детерминанты и способы борьбы с ней.

Работа предназначена для курсантов, слушателей, студентов юридических ВУЗов, преподавателей, сотрудников правоохранительных органов.

УДК 34С5
ББК 67.99(2)8

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

С середины прошлого века философами обсуждается вопрос о вступлении человечества в качественно новую стадию социального развития, именуемую постиндустриальным или информационным обществом, явившуюся результатом информационно-технологической революции[1]. Информация стала первоосновой жизни современного общества, продуктом общественных отношений, приобрела товарные черты и стала предметом купли-продажи.

Вместе с тем информационные процессы не только открыли новые, ранее не известные возможности для прогрессивного развития человечества, но и вызвали одновременно ряд качественно новых угроз, в том числе и глобального значения. Возник новый вид преступных посягательств, связанных с использованием средств компьютерной техники. Это обусловило появление потребности в защите информации, в том числе и особого ее вида – компьютерной информации.

Сегодня в компьютерных системах обрабатывается значительный объем различной информации, и с каждым днем область применения информационных компьютерных технологий расширяется. Все это предопределило то, что борьба с преступлениями в сфере компьютерной информации остается одной из актуальных проблем в мире. В этом плане Россия, в которой отмечается ежегодное увеличение числа зарегистрированных преступлений в сфере компьютерной информации, не является исключением. Количество регистрируемых преступлений в сфере компьютерной информации представляет собой стабильно неуклонно растущую кривую, и хотя их удельный вес в общем числе зарегистрированных преступлений составляет десятую долю процента, обращают на себя темпы роста преступности данного вида. Зарегистрированная преступность в сфере компьютерной информации лишь частично отражает реальное состояние изучаемого вида преступности, которое в несколько раз превышает данные официальной статистики и свидетельствует об исключительно высоком уровне его латентности[2].

Актуальность данной темы определяется также той опасностью и распространенностью, которую за последние 40 лет приобрело такое явление, как незаконный оборот вредоносных компьютерных программ. За последние 12 лет, начиная с 2000 года, количество зарегистрированных преступлений, предусмотренных ст. 273 УК РФ, увеличилось более чем в 10 раз. Кроме того, положение усугубляется тем, что преступления, связанные с незаконным оборотом вредоносных компьютерных программ, совершаются новым типом преступника, ранее не попадавшем в поле зрения правоохранительных органов.

Некоторые из вредоносных программ, выходя из-под контроля своих создателей, могут неуправляемо наносить огромный ущерб охраняемым законом общественным отношениям. Особое место среди этих программ занимают вирусы. Количество известных вирусов не поддается строгому учету и постоянно увеличива-

---

[1] См. например: Воронина Т. П. Информационное общество: сущность, черты, проблемы. М., 1995; Кастельс М. Информационная эпоха. Экономика, общество и культура. М., 2000.

[2] См.: Айков Д. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями / Д. Айков, К. Сейгер, У. Фонсторх. М.: Мир, 1999. С. 18; Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография. М.: Норма, 2004. С. 125.

ется. Каждый месяц в России появляется более 4 тысяч новых вирусов, которые все чаще создаются не хакерами-самоучками, а организованными преступными группами, с целью извлечения коммерческой выгоды.

Специфичность преступлений, связанных с незаконным оборотом вредоносных компьютерных программ, многообразие способов преступных посягательств, недостаточная разработанность теоретической модели таких преступлений, создают существенные преграды в борьбе с ними, что требует интенсивной научной проработки данной проблемы.

Все вышеизложенное подтверждает актуальность данной темы и открывает широкое поле для исследовательской деятельности в сфере незаконного оборота вредоносных компьютерных программ, в целях выявления проблемных моментов, повышения эффективности противодействия изучаемому виду преступности и формулирования конкретных предложений по совершенствованию законодательства в этой области.

УГОЛОВНО-ПРАВОВАЯ И КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПНОСТИ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

1.1. Понятие преступлений в сфере компьютерной информации

Бурное развитие компьютерной техники и информационных технологий послужило толчком к развитию общества, построенного на использовании различного рода информации и получившего название информационного общества. Эта революция, как и предшествующие ей в истории общества революции (аграрная и промышленная), повлекла за собой серьезные социальные изменения, наиболее важными из которых является появление нового вида общественных отношений и общественных ресурсов – информационных. Последние отличаются от известных ранее целым рядом особенностей, а именно:

- они не потребляемы и подвержены не физическому, а моральному износу;

- они по своей сущности нематериальны и несводимы к физическому носителю, в котором воплощены;

- их использование позволяет резко сократить потребление остальных видов ресурсов, что в конечном итоге приводит к колоссальной экономии средств;

- процесс их создания и использования осуществляется особым способом – с помощью компьютерной техники[3].

Информация стала первоосновой жизни современного общества, продуктом общественных отношений, приобрела товарные черты и стала предметом купли-продажи.

Однако, совершенствование технологий приводит не только к развитию информационного общества, но и к появлению новых, ранее не известных источников опасности для него. Обороноспособность и экономика многих государств мира становятся все более зависимыми от нормального функционирования компьютерных сетей, нарушение работоспособности которых может повлечь серьезные последствия. Небольшая компьютерная программа может при определенных обстоятельствах причинить более существенный ущерб, чем взрыв бомбы. При этом затраты на реализацию «компьютерного» нападения и риск быть в дальнейшем обнаруженным, как правило, несоизмеримо ниже, чем для «традиционных» видов террористических действий[4].

По всей видимости, первое в истории человечества компьютерное преступление было совершено в 1801 году, когда французский инженер Жозеф Жаккар создал с целью повышения прибыли прообраз компьютерной перфокарты и оснастил шелкоткацкие станки простейшими устройствами для снятия с нее информации. Это устройство позволяло повторять серию операций в про-

---

[3] Савельева И.В. Правовая охрана программного обеспечения ЭВМ // Право и информатика. М.: МГУ, 1990. С. 9.

[4] Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография. М.: Норма, 2004. С. 6.

цессе изготовления специальных тканей. Служащие Жаккара были настолько обеспокоены угрозой потери работы, что совершили массовые акты саботажа с целью помешать использованию в дальнейшем новой технологии[5].

Созданные в середине XX века первые компьютеры были предназначены для решения различных научных задач и эксплуатировались только в закрытых научных учреждениях. Поэтому доступ к компьютерной информации со стороны был практически невозможен.

С появлением и увеличением числа персональных компьютеров стали иметь место различные злоупотребления и нарушения правил работы с компьютерной информацией, установленных внутриведомственными нормативными документами. Однако, проблема охраны информации не выходила за пределы государственных границ.

Первые случаи преступлений, совершенных с использованием ЭВМ, были выявлены в начале 60-х годов в США. А первое преступление, совершенное с использованием компьютера в бывшем СССР, было зарегистрировано в 1979 г. в Вильнюсе: им явилось хищение, ущерб от которого составил 78584 руб. Данный факт был занесен в международный реестр правонарушений подобного рода и явился своеобразной отправной точкой в развитии нового вида преступлений в нашей стране[6].

Рост количества ЭВМ, стремительная компьютеризация, захватившая практически все стороны жизнедеятельности общества, возникновение потребности в информационном обмене предопределило необходимость создания компьютерных сетей. Зарождение прообраза сети Интернет произошло в 1961 году, когда в рамках реализации одного из проектов Агентства передовых исследований Министерства обороны США (Advanced Research Agency – ARPA) была создана сеть ARPANET. Уже в первые годы использования сети среди ее пользователей были достаточно распространены розыгрыши, которые были связаны с незначительными нарушениями предусмотренных правил обеспечения безопасности. Поскольку число пользователей было небольшим и все они, как правило, были знакомы и доверяли друг другу, подобные несанкционированные подключения не рассматривались в то время в качестве противоправных действий. Первым крупным инцидентом, связанным с функционированием сети, принято считать выявленное и описанное К. Столлом проникновение в сеть извне, которое совершил иностранный хакер. В своей книге К. Столл впервые привлек внимание общественности к возможности использования сетей в противоправных целях[7].

Сегодня сеть Интернет нельзя считать безопасным местом. Интернет активно развивается и уже сейчас в полной мере применяется для связи, коммерции, финансовой деятельности.

Основным средством борьбы с преступлениями в данной сфере, на наш взгляд, должно быть уголовное законодательство. В странах с наиболее высо-

---

[5] Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: ООО Издательство «Юрлитинформ», 2002. С. 16.

[6] Батурин Ю.М. Проблемы компьютерного права. М.: Юридическая литература, 1991. С. 126.

[7] Осипенко А.Л. Указ. соч. С. 27.

ким уровнем технического и экономического развития процесс его формирования идет уже не один десяток лет[8]. Между тем на практике наблюдается существенное различие в подходах к проблеме борьбы с компьютерной преступностью. Например, в то время как в ряде стран (Китае, Саудовской Аравии и др.) использование глобальных компьютерных сетей находится под практически полным государственным контролем, то до сих пор есть государства, где вообще отсутствуют законы, устанавливающие ответственность за компьютерные преступления.

Наиболее развитая система правовых норм, регулирующих отношения в рассматриваемой сфере, к настоящему моменту сформирована в США, где ответственность за компьютерные преступления устанавливается на двух уровнях - на федеральном и на уровне штатов. На уровне федерации все компьютерные преступления включены в § 1030 Титула 18 Свода законов США. На уровне штатов принимаются отдельные законы по вопросам компьютерной преступности. Одним из первых принял свой Закон в 1978 г. штат Флорида. Он устанавливал ответственность за модификацию, уничтожение и несанкционированный доступ к компьютерной информации. В штате Техас в 1985 г. принят Закон о компьютерных преступлениях (Texas Computer Crimes Law), по которому наказывалось незаконное использование компьютерной информации, незаконное проникновение в компьютерную сеть.

В Великобритании ответственность за компьютерные преступления установлена в статутах, принятых Парламентом. Их можно подразделить на две основные группы: статуты, устанавливающие ответственность за компьютерные преступления (собственно computer crime), и статуты, устанавливающие ответственность за преступления, связанные с использованием Интернета (internet-related crime). Однако термин computer crime употребляется лишь в доктрине, в законодательстве же используется термин computer misuse. Дословно термин «misuse» переводится как «неправильное употребление, плохое обращение, злоупотребление». В большинстве русских источников название закона, в котором употребляется этот термин, - Computer Misuse Act 1990 - переводится как Закон о злоупотреблении компьютером[9]. К статутам, регулирующим правонарушения в информационной сфере, можно отнести, наряду с Законом о злоупотреблении компьютером 1990 г. (Computer Misuse Act 1990), Закон о телекоммуникациях (обман) 1997 г. (Telecommunications (Fraud) Act 1997), Закон о защите данных 1998 г. (Data Protection Act 1998) и Закон об электронных коммуникациях 2000 г. (Electronic Communications Act 2000).

Заслуживающие внимание нормы, определяющие составы компьютерных преступлений, содержатся также в уголовном законодательстве Канады, Германии, Испании, Швейцарии, Нидерландов, Японии и других государств. Определенный опыт законодательного регулирования в уголовном праве вопросов

---

[8] См. подробнее: Борчева Н.А. Компьютерное право и ответственность за компьютерные преступления за рубежом // На пути к информационному обществу: криминальный аспект: Сборник статей. М., 2002. С. 15; Ястребов Д.А. Институт уголовной ответственности в сфере компьютерной информации (опыт международно-правового сравнительного анализа) // Государство и право. 2005. № 1. С. 53-63.

[9] Степанов-Егиянц В. Ответственность за компьютерные преступления // Законность. 2005. № 12. С. 49.

ответственности за совершение преступлений в сфере компьютерной информации накоплен государствами-участниками СНГ.

Первой попыткой решить вопрос законодательного закрепления правоотношений, вытекающих из различных сфер применения средств автоматической обработки информации в России стала разработка в 1991г. проекта Закона РСФСР «Об ответственности за правонарушения при работе с информацией», который предусматривал основания для дисциплинарной, гражданско-правовой, административной, уголовной ответственности за подобные деяния. Однако он так и не был принят, главным образом, из-за общей неразработанности законодательного поля в данной области права.

В 1992 году были приняты два закона: Закон РФ «О правовой охране программ для электронных вычислительных машин и баз данных», который содержал положение о том, что выпуск под своим именем чужой программы для ЭВМ или базы данных либо незаконное воспроизведение или распространение таких продуктов влечет за собой уголовную ответственность; и Закон РФ «О правовой охране топологий интегральных микросхем»[10].

В последующие годы высшие органы власти уделяли повышенное внимание вопросам упорядочения отношений в сфере информации. Были приняты законы «Об авторском праве и смежных правах»[11], «О государственной тайне»[12], «О связи»[13], «Об электронной цифровой подписи»[14], «Об участии в международном информационном обмене»[15].

Важное место в ряду нормативно-правовых актов в области компьютерного права занял Федеральный закон «Об информации, информатизации и защите информации»[16] 1995 года, давший определение многих терминов данной сферы деятельности. Этот закон подготовил правовое поле для принятия нового уголовного законодательства и формирования самостоятельной отрасли права – компьютерного права[17].

Мировая уголовно-правовая практика в зависимости от традиций законодательства той или иной страны для криминализации новых разновидностей преступлений идет двумя путями: или дополняет традиционные составы преступлений новыми аспектами, или формирует новые нормы и институты права, объединенные единым специфичным объектом преступления. Российское уголовное право и законодательство всегда шли по второму из названных путей развития, беря за основу криминализации новых разновидностей преступлений признак их объекта. Хотя в юридической литературе встречаются и другие мнения. Например, Ю.М. Батурин и А.М. Жодзишский предлагали объединить

---

[10] Ведомости Съезда народных депутатов РФ и Верховного Совета РФ. 1992. № 42. Ст. 2325, 2328. (Утратили силу в связи с принятием Федерального закона от 18.12.2006 №231-ФЗ.)

[11] Ведомости Съезда народных депутатов РФ и Верховного Совета РФ. 1993. № 32. Ст. 1242. (Утратил силу в связи с принятием Федерального закона от 18.12.2006 №231-ФЗ.)

[12] Российская газ. 1993. 21 сент.

[13] Собрание законодательства РФ. 2003. № 28. Ст. 2895.

[14] Собрание законодательства РФ. 2002. № 2. Ст. 127.

[15] Собрание законодательства РФ. 1996. № 28. Ст. 3347.

[16] Собрание законодательства РФ. 1995. № 8. Ст. 609. (Утратили силу в связи с принятием Федерального закона от 27.07.2006 №149-ФЗ.)

[17] См.: Скоромников К.С. Компьютерное право Российской Федерации: Учебник. М., 2000.

оба пути, введя в Уголовный кодекс три самостоятельные статьи: «Несанкционированный доступ в компьютерную систему», «Угроза возникновения конфликта» и «Заражение компьютерным вирусом», а ряд других статей дополнив квалифицирующим признаком использования средств компьютерной техники[18].

С появлением в первой половине 1990-х гг. проблемы внесения в УК России компьютерных преступлений, возник вопрос выбора их места в системе Особенной части УК РФ. Разработчики первого проекта криминализации компьютерных преступлений относили данные деяния к хозяйственным преступлениям.

Второй проект криминализации преступлений в области компьютерной информации разрабатывался исходя из задачи их формирования в новом Уголовном кодексе. Было опубликовано два варианта проекта УК, которые уже содержали в себе самостоятельную главу «Компьютерные преступления» (29-ю по проекту 1994 г., 28-ю – по проекту 1995 г. и далее)[19].

Заслугой авторов явилось верное определение родового объекта рассматриваемого вида деяний и помещение этой группы преступлений в рамки раздела IX «Преступления против общественной безопасности и общественного порядка».

Оба проекта главы достаточно тесно повторяли друг друга и включали в себя следующие пять составов преступлений: самовольное проникновение в автоматизированную компьютерную систему; неправомерное завладение программами для ЭВМ, файлами или базами данных; самовольная модификация, повреждение, уничтожение баз данных или программ для ЭВМ; внесение или распространение вирусных программ для ЭВМ; нарушение правил, обеспечивающих безопасность информационной системы.

Из анализа текстов статей видно, что при некоторых различиях в их последовательности расположения в главе и в используемой терминологии их количество и сущность остались теми же. Поэтому и после опубликования данных проектов юристами и специалистами в области информационных технологий было указано на существенные недостатки, в частности, на отсутствие единой правовой концепции в главе, недостаточную связь с отраслевыми законами, слабую проработку терминологии и стилистики[20].

После доработки проекта с учетом высказанных замечаний, к началу 1996 г. глава предстала в следующем виде:

Глава 28. Преступления в сфере компьютерной информации.

Статья 268. Неправомерный доступ к компьютерной информации.

Статья 269. Создание, использование и распространение вирусных программ.

---

[18] Батурин Ю.М. Компьютерная преступность и компьютерная безопасность / Ю.М. Батурин, А.М. Жодзишский. М.: Юридическая литература, 1991. С. 28; См. также: Добровольский Д.В. Актуальные проблемы борьбы с компьютерной преступностью. Уголовно-правовые и криминологические аспекты: Дис. … канд. юрид. наук. М., 2005.

[19] См.: Уголовный кодекс РФ. Особенная часть: Проект // Юридический вестник. 1994. № 22-23; Уголовный кодекс РФ: Проект // Юридический вестник. 1995. № 7-8.

[20] См.: Максимов В.Ю. Незаконное обращение с вредоносными программами для ЭВМ: проблемы криминализации, дифференциации ответственности и индивидуализации наказания: Дис. … канд. юрид. наук. Краснодар, 1998.

Статья 270. Нарушение правил эксплуатации компьютерной системы или сети.

В главу были внесены значительные изменения, и в первую очередь они коснулись ее названия: расплывчатое криминологическое было заменено на более точное уголовно-правовое.

Однако и на этом работа над главой 28 УК РФ не была остановлена, и после ее окончательной доработки глава предстала в конечном варианте. В статье 268 УК РФ «Неправомерный доступ к компьютерной информации» был декриминализирован доступ к любой информации ЭВМ, а предметом преступления стали только данные, охраняемые законом. Также частично было декриминализировано нарушение правил эксплуатации ЭВМ (ст. 274): в качестве предмета деяния стала рассматриваться только машинная информация, охраняемая законом; обязательным итогом этого преступного деяния был назван «существенный вред». Наконец, произошли изменения и в статье о вирусном преступлении: понятие «вирус» в названии статьи было заменено на понятие «вредоносная программа для ЭВМ»; субъективная сторона создания таких программ была дополнена признаком заведомости их вредоносных свойств для виновного, что подчеркнуло прямой характер умышленной вины преступления; предметом использования и распространения, кроме программ, стали также машинные носители с ними; максимальный размер основного наказания санкции ч. 1 был несколько снижен – с 4 до 3 лет лишения свободы.

В этом виде глава 28 УК РФ существовала до 2011 года, когда, наконец, в данную главу были внесены изменения, наиболее соответствующие требованиям современности.

Безусловным достоинством новой редакции диспозиции статей 272-273 УК РФ явилась замена термина «ЭВМ» на «компьютер». В предыдущей редакции статей термин «компьютер» употребляется в том же смысле, что и термин «ЭВМ», что на наш взгляд, является не совсем правильным. Данные термины не являются синонимами. С начала 1990-х годов термин «компьютер» вытеснил термин «электронная вычислительная машина» (ЭВМ), который, в свою очередь, в 1960-х годах заменил понятие «цифровая вычислительная машина» (ЦВМ). В толковом словаре английского языка компьютер определяется как совокупность аппаратно-технических средств, позволяющих производить операции над символьной и образной информацией[21]. Иначе говоря, это – электронная цифровая машина, являющаяся универсальным средством управления, автоматизации, обработки данных, которыми могут быть не только числа, но и всевозможные тексты, сигналы, изображения, представленные в цифровой форме. Термин ЭВМ означает электронную машину, предназначенную преимущественно для решения вычислительных задач. Поэтому, на наш взгляд, более правильным было бы употребление терминов «компьютер», «компьютерная система», «компьютерная сеть».

---

[21] См. например: Хокинс Дж.М. The Oxford dictionary of the English Language (Оксфордский толковый словарь английского языка). Oxford University Press, Астрель, АСТ, 2001. Русско-английский толковый словарь по информатике / В.И. Першиков, А.С. Марков, В.М. Савинков, 3-е изд. М.: Финансы и статистика, 1999.

Под компьютером, на наш взгляд, следует понимать – комплекс электронных устройств, производящих заданные программой операции, обеспечивающие протекание информационных процессов и управление периферийными устройствами.

Особенностью компьютера является то, что процессы обработки данных происходят внутри нее и не отделимы от нее, поэтому в широком смысле компьютер является совокупностью трех составляющих его элементов: аппаратной части; программной части; информации[22].

На сегодняшний день, с момента включения главы 28 в УК РФ 1996 года, уже успела сложиться не только определенная практика, но и выработаться определенная научная позиция по компьютерным преступлениям. В то же время вопрос о терминологии в сфере компьютерных преступлений и даже вопрос о правильности названия самой главы 28 УК продолжает оставаться открытым. Между тем это принципиальный вопрос, поскольку в зависимости от применяемой терминологии соответствующий институт будет наполняться различным содержанием. Следует отметить, что терминология в сфере компьютерных технологий в силу своей относительной молодости не устоялась и не получила четкого закрепления даже в специальных науках, например кибернетике. Тем более сложно приходится специалистам в области права, так как право требует строгих определений, которые должны быть основаны на разработках соответствующих наук.

В российской науке уголовного права достаточно часто употребляется термин «компьютерные преступления», который, однако не используется в Уголовном Кодексе РФ. До сих пор в отечественной юридической науке нет однозначного мнения, что следует понимать под данным термином. Это обусловлено отсутствием единообразной доктринальной позиции по отнесению конкретных противоправных деяний к таким преступлениям в связи с постоянными изменениями информационных компьютерных технологий.

Анализ существующих подходов к определению дефиниции «компьютерное преступление» позволяет выделить несколько устоявшихся подходов.

Сторонники одного подхода отрицают компьютерные преступления как самостоятельный вид преступлений, поскольку использование компьютеров может являться особенностью или квалифицирующим признаком различных общеуголовных преступлений[23]. Один из основных аргументов в пользу такой точки зрения: преступления не принято дифференцировать по видам технических средств, с помощью которых они совершаются.

Приверженцы другого подхода допускают существование такой формулировки, поскольку данный термин уже прочно вошел в международную профес-

---

[22] См.: Максимов В.Ю. Незаконное обращение с вредоносными программами для ЭВМ: проблемы криминализации, дифференциации ответственности и индивидуализации наказания: Дис. … канд. юрид. наук. Краснодар, 1998.

[23] Батурин Ю.М. Проблемы компьютерного права. М.: Юридическая литература, 1991. С. 271; Батурин Ю.М. Компьютерная преступность и компьютерная безопасность / Ю.М. Батурин, А.М. Жодзишский. М.: Юрид. лит., 1991. С. 11.

сиональную лексику[24]. При этом, как правило, отмечается, что хотя понятие «компьютерные преступления» нельзя использовать строго в уголовно-правовом значении, однако его употребление целесообразно в криминологическом и криминалистическом аспектах, то есть когда речь идет о личности преступника или способе совершения преступления.

Сторонники третьей позиции полагают, что в строго юридическом смысле термин «компьютерное преступление» весьма уязвим, поэтому предлагается заменить его другим термином – «информационное преступление», под которым следует понимать запрещенные УК общественно опасные деяния, объектом преступных посягательств которых являются информационные правоотношения в информационной сфере. При этом предметом преступных посягательств является охраняемая законом информация, в том числе и на машинных носителях[25]. В.В. Крылов отмечает, что употребление понятия «информационные преступления» в качестве базового позволяет абстрагироваться от конкретных технических средств, используемых участниками правоотношений в области информационной деятельности, и дает возможность оценить действующие в ней закономерности[26]. Термин «информационные преступления» представляется нам не совсем удачным, так как в информационных преступлениях предметом будет любая информация, а не обязательно информация на машинных носителях. Следовательно понятие «информационное преступление» будет весьма размытым, а его применение противоречивым.

Законодатель не дает определения компьютерного преступления, но выделенную группу однородных преступлений, посягающих на один и тот же объект уголовно-правовой охраны, определяет термином «преступления в сфере компьютерной информации», который используется не только в российском законодательстве, но и на международном уровне. Так в Соглашении о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации, термин «преступления в сфере компьютерной информации» раскрывается как «уголовно наказуемое деяние, предметом которого является компьютерная информация»[27].

Могут ли эти термины «компьютерное преступление» и «преступление в сфере компьютерной информации» использоваться как синонимы? Некоторые ученые рассматривают их таковыми[28]. На наш взгляд, использовать термин

---

[24] Вехов В.Б. Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники. М.: ЦИнНМОКП МВД России, 2000. С 6; Ляпунов Ю. Ответственность за компьютерные преступления / Ю. Ляпунов, В. Максимов // Законность. 1997. № 1. С. 9; Максимов В.Ю. Незаконное обращение с вредоносными программами для ЭВМ: проблемы криминализации, дифференциации ответственности и индивидуализации наказания: Дис. ... канд. юрид. наук. Краснодар, 1998. С. 33; Селиванов Н. Проблемы борьбы с компьютерной преступностью // Законность. 1993. № 8. С. 37.

[25] Пархомов В.А. К определению понятия «Информационное преступление» // Вестник ИГЭА. 2001. № 2. С.10; См.: Дворецкий М.Ю. Преступления в сфере компьютерной информации (уголовно-правовое исследование): Дис. … канд. юрид. наук. Волгоград. 2001; Крылов В. В. Расследование преступлений в сфере информации. М., 1998. С. 162.

[26] Крылов В.В. Информационные компьютерные преступления. М.: Изд. Группа ИНФА-М-НОРМА, 1997. С. 10-11.

[27] Бюллетень международных договоров. 2002. № 11.

[28] Гаджиев М.С. Криминологический анализ преступности в сфере компьютерной информации (по материалам республики Дагестан): Автореф. дис. … канд. юрид. наук. Махачкала, 2004. С. 9.

«компьютерные преступления» в отношении деяний, предусмотренных главой 28 УК РФ можно лишь с большой долей условности. Термин «компьютерное преступление» является более широким, скорее ассоциативным. К подобным преступлениям можно отнести не только преступления, перечисленные в главе 28 УК РФ, но и те преступления, которые совершены с использованием компьютерных технологий. А лица, совершившие подобные деяния должны привлекаться к уголовной ответственности по совокупности преступлений.

В настоящей работе термин «компьютерные преступления» будет использоваться так, как это принято в международной практике – в криминолого-криминалистическом смысле.

В отечественной юридической литературе предпринято достаточно большое количество попыток дать определение понятию «преступление в сфере компьютерной информации».

Так, по мнению С.Г. Спириной, преступление в сфере компьютерной информации – это «предусмотренное уголовным законом, противоправное, виновное нарушение чужих прав и интересов, связанное с использованием, модификацией, уничтожением компьютерной информации, причинившее вред либо создавшее угрозу причинения вреда подлежащим уголовно-правовой охране правам и интересам физических и юридических лиц, общества и государства (личным правам и неприкосновенности частной сферы, имущественным правам и интересам, общественной и государственной безопасности в области высоких технологий и конституционному строю)»[29]. В данном определении не указаны такие признаки, как общественная опасность и наказуемость деяния.

В.С. Карпов считает, что «преступление в сфере компьютерной информации – это запрещенное уголовным законом, совершенное виновно общественно опасное деяние, посягающее на нормальный порядок развития отношений в сфере компьютерной информации и безопасное функционирование ЭВМ, системы ЭВМ или их сети»[30]. В предложенной формулировке отсутствует указание на последствия и на наказуемость деяния.

В.А. Бессонов даёт следующее определение данному виду преступлений: «предусмотренное уголовным законом виновное нарушение чужих прав и интересов в отношении автоматизированных систем обработки данных, совершенное во вред подлежащим правовой охране имущественным правам и интересам, общественной и государственной безопасности и конституционному строю»[31]. К недостаткам данного определения можно отнести отсутствие указания на такие признаки как общественная опасность и наказуемость.

По мнению М.С. Гаджиева «под преступлениями в сфере компьютерной информации следует понимать предусмотренный уголовным законом противоправный, виновный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для ЭВМ, а также

---

[29] Спирина С.Г. Криминологические и уголовно-правовые проблемы преступлений в сфере компьютерной информации: Дис. ... канд. юрид. наук. Краснодар, 2000. С. 69.

[30] Карпов В.С. Уголовная ответственность за преступления в сфере компьютерной информации: Дис. … канд. юрид. наук. Красноярск, 2002. С. 43.

[31] Бессонов В.А. Виктимологические аспекты предупреждения преступлений в сфере компьютерной информации: Дис. ... канд. юрид. наук. Н. Новгород, 2000. С. 37.

нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сетей, связанное с использованием, модификацией, уничтожением компьютерной информации»[32]. Представляется, что привязка данного определения к тексту статей главы 28 УК РФ ограничивает круг преступлений в сфере компьютерной информации.

Т. Г. Смирнова полагает, что «преступления в сфере компьютерной информации – это запрещенные уголовным законом общественно-опасные виновные деяния, которые, будучи направленными на нарушение неприкосновенности охраняемой законом компьютерной информации и ее материальных носителей (в частности, компьютерной техники (ЭВМ), систем ЭВМ или их сетей), причиняют либо создают угрозу причинения вреда жизни и здоровью личности, правам и свободам человека и гражданина, государственной и общественной безопасности»[33]. К недостаткам определения можно отнести то, что указанный текст содержит целый ряд терминов, не закрепленных в УК РФ и требующих от автора дополнительного разъяснения их содержания.

Попытаемся дать определение понятия «преступление в сфере компьютерной информации». Для этого необходимо правильно определить объект преступного посягательства.

В отечественной уголовно-правовой литературе нет существенных разногласий по поводу определения родового объекта преступлений в сфере компьютерной информации. Родовой объект преступлений, закрепленных в главе 28 УК РФ, предопределен самим фактом размещения этой главы в разделе «Преступления против общественной безопасности и общественного порядка». Последствия неправомерного использования компьютерной информации могут быть самыми разнообразными: это не только нарушение неприкосновенности интеллектуальной собственности, но и разглашение сведений о частной жизни граждан, имущественный ущерб в виде прямых убытков и неполученных доходов, потеря репутации фирмы, различные виды нарушений нормальной деятельности предприятия, отрасли и т.д.[34] Таким образом, законодатель определил родовой объект компьютерных преступлений как отношения общественной безопасности и общественного порядка. Данный родовой объект составляют такие общественные ценности как: общественная безопасность, общественная нравственность, здоровье населения, экологическая, транспортная безопасность, безопасность в сфере обращения компьютерной информации. Последняя составляющая родового объекта и составляет видовой объект компьютерных преступлений.

По поводу определения видового объекта преступлений в сфере компьютерной информации в отечественной юридической литературе существуют несколько точек зрения. Так, С.Н. Никулин видовым объектом считает общественные отношения по обеспечению безопасности информации и компьютерных систем[35]. Т.Г. Смирнова – специальную группу общественных отношений, содержание

---

[32] Гаджиев М.С. Криминологический анализ преступности в сфере компьютерной информации (по материалам республики Дагестан): Дис. … канд. юрид. наук. Махачкала, 2004. С. 20.

[33] Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: Дис. … канд. юрид. наук. М., 1998. С. 40.

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

[35] Уголовное право России. Особенная часть: Учебник / Под ред. А.И. Рарога. М.: Триада-ЛТД Ю, 1996. С. 323.

которых составляют права и интересы различных субъектов в области обеспечения безопасности использования информации и информационных ресурсов, необходимых для нормальной жизнедеятельности социума[36]. В.Ю. Максимов – совокупность общественных отношений по правомерному и безопасному использованию информации[37]. И. А. Клепицкий рассматривает видовой объект как часть установленного порядка общественных отношений, связанных с производством различных операций с компьютерной информацией[38]. В.С. Комиссаров к видовому объекту относит совокупность общественных отношений по безопасному производству, хранению, использованию или распространению информации и информационных ресурсов либо их защиты[39]. По мнению Т.М. Лопатиной видовым объектом преступлений в сфере компьютерной информации являются общественные отношения, связанные с реализацией различными лицами права на безопасность информации, представленной в особом (электронном) виде[40].

Во всех приведенных определениях речь идет о соблюдении прав и законных интересов различных субъектов – пользователей компьютеров, компьютерных систем и их сетей в сфере безопасного пользования компьютерной информацией. Сфера компьютерной информации является частью информационной сферы. Информационная сфера, в свою очередь, определяется как область деятельности субъектов, связанная с созданием, преобразованием и потреблением информации[41].

Нам представляется, что видовым объектом преступлений в сфере компьютерной информации является совокупность общественных отношений, обеспечивающих безопасное создание, преобразование, потребление и защиту компьютерной информации, необходимых для нормальной жизнедеятельности общества.

Для оценки характера и степени общественной опасности деяния и его правильной квалификации важно уяснить особенности непосредственного объекта преступления в сфере компьютерной информации. Как следует из теории уголовного права, непосредственным объектом является какое-либо отдельно взятое общественное отношение, сущность которого состоит в охране уголовно-правовой нормой возможности действовать определенным образом или пребывать в известном состоянии[42]. Для каждого состава преступлений главы 28 УК РФ существует свой непосредственный объект[43]. Анализ статей 272-274 УК РФ показывает, что непосредственным объектом преступлений в сфере компьютерной информации выступают общественные отношения, обеспечивающие:

---

[36] Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: Автореф. дис. … канд. юрид. наук. М., 1998. С. 12.

[37] Ляпунов Ю. Указ. соч. С. 9.

[38] Уголовное право России. Особенная часть: Учебник / Под ред. Б.В. Здравомыслова. М.: Юрист, 1996. С. 350.

[39] Комиссаров В. С. Преступления в сфере компьютерной информации: понятие и ответственность // Юридический мир. 1998. № 2. С. 11.

[40] Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: Дис. … д-ра юрид. наук. М., 2006. С. 195.

[41] См.: Об информации, информатизации и защите информации: Федеральный закон от 20.02.1995 № 24-ФЗ // СЗ РФ. 1995. № 8. Ст. 609; Об участии в информационном обмене: Федеральный закон от 04.07.1996 // СЗ РФ. 1996. № 28. Ст. 3347.

[42] Лопатина Т.М. Указ. соч. С. 196.

[43] Ляпунов Ю. Указ. соч. С. 11-14; Российское уголовное право. Особенная часть / Под ред. В.Н. Кудрявцева и А.В. Наумова. М., 1997. С. 350-352.

- для ст. 272 УК РФ – безопасность охраняемой законом компьютерной информации;

- для ст. 273 УК РФ – любой компьютерной информации, хранимой и обрабатываемой в компьютере, компьютерной системе или сети;

- для ст. 274 УК РФ – безопасность эксплуатации компьютера, компьютерной системы или сети.

В юридической литературе высказывались мнения о том, что рассматриваемые преступления, посягая на основной объект, всегда причиняют вред и дополнительному: личным правам и неприкосновенности частной сферы, имущественным правам, государственной безопасности и др.[44] Однако, дополнительный объект будет таковым только до тех пор, пока опасность по отношению к нему менее велика, чем к основному объекту. В противном случае возможны два варианта квалификации такого сложного преступления: 1) если последствия наступают по неосторожности, они могут быть закреплены в данной статье как отягчающее обстоятельство; 2) если они охватывались умыслом виновного, необходимо оценивать содеянное по правилам идеальной совокупности преступлений[45].

Кроме того, преступления в сфере компьютерной информации имеют общий предмет преступного посягательства. Им, по мнению подавляющего большинства ученых, является компьютерная информация. Одни ученые определяют компьютерную информация как информацию, зафиксированную на машинном носителе и передаваемую по телекоммуникационным каналам в форме, доступной восприятию ЭВМ[46]. Другие под компьютерной информацией понимают совокупность сведений, представляющих особую ценность для государства, общества и отдельных граждан, производство, хранение и использование которых осуществляется посредством компьютерной техники[47].

В некоторых публикациях высказываются мнения, что компьютерная информация является объектом подобных преступлений[48]. Мы будем исходить из того, что объектом преступления могут быть лишь соответствующие общественные отношения, а информация, обрабатываемая и используемая в компьютерных системах, является предметом преступления, хотя довольно специфическим.

Для правильного понимания специфики предмета преступлений в сфере компьютерной информации целесообразно рассмотреть ряд существенных обстоятельств, характеризующих правовой режим компьютерной информации в Российской Федерации.

Прежде всего, отметим, что согласно ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[49], информация – это сведения (сообщения, данные) независимо от формы их представления.

---

[44] Уголовное право России. Особенная часть: Учебник / Под ред. Б. В. Здравомыслова. М.: Юрист, 1996. С. 351.
[45] Максимов В. Ю. Указ. соч. С. 88.
[46] Комментарий к Уголовному кодексу Российской Федерации. Изд. 3-е, изм. и доп. / Под общей ред. Ю.И. Скуратова, В. М. Лебедева. М.: Издательская группа НОРМА – ИНФА, 1999. С. 696.
[47] Смирнова Т. Г. Указ. соч. С. 11.
[48] Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия. М., 1996. С.17.
[49] См.: Собрание законодательства РФ. 2006. № 31(1ч.). Ст. 3448.

Основной единицей такой информации является документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством РФ случаях ее материальный носитель[50].

Информационные технологии, в соответствии с п. 2 ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации», это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информация, в том числе и компьютерная, обращается в информационной сфере, которая согласно ст. 1 Федерального закона «Об информации, информационных технологиях и о защите информации», представляет собой совокупность отношений, возникающих при осуществлении права на поиск, получение, передачу, производство и распространение информации; применении информационных технологий; обеспечении защиты информации.

Таким образом, сфера компьютерной информации, как составная часть информационной сферы, является многоуровневой, и в самом общем виде включает в себя отношения, возникающие по поводу:

- поиска, получения, передачи, производства и распространения компьютерной информации;
- применения информационных компьютерных технологий;
- обеспечения защиты компьютерной информации.

Компьютерная информация имеет специфику, которую можно свести к следующему:

- данная информация очень объемна и быстро обрабатываема;
- компьютерная информация очень легко и, как правило, бесследно уничтожаема;
- данный вид информации может находиться лишь на машинном носителе;
- компьютерная информация может создаваться, изменяться, копироваться, использоваться только с помощью компьютера, компьютерной системы или сети;
- эта информация легко передается по телекоммуникационным каналам связи компьютерных сетей, причем практически любой объем информации можно передать на любое расстояние.

Кроме того, можно отметить относительную простоту в пересылке, преобразовании, размножении компьютерной информации; при изъятии информации, в отличие от изъятия вещи, она легко сохраняется в первоисточнике; доступ к одному и тому же файлу, содержащему информацию, могут иметь одновременно несколько пользователей.

В описании предмета преступного посягательства в сфере компьютерной информации законодатель использует разные формулировки: «охраняемая за-

[50] См.: Собрание законодательства РФ. 2006. № 31 (1ч.). Ст. 3448.

коном компьютерная информация» (ст. 272 УК), «информация» (ст. 273 УК), «охраняемая законом компьютерная информация» (ст. 274 УК). Анализ текста ст. 273 УК РФ, где при упоминании термина «информация» снято указание на ее охраняемость законом, показывает, что в данном случае, уголовно-правовой защите подлежит любая информация, независимо от того, имеет ли она собственника (законного владельца) или предназначена для использования неограниченным кругом лиц. Тем самым подчеркивается общественная опасность действий с вредоносными программами. При совершении двух других преступлений в сфере компьютерной информации (статьи 272, 274 УК) уголовно-правовой защите подлежит документированная охраняемая законом информация, способ использования которой установлен собственником или законным владельцем.

Давая определение информации и выделяя документированную информацию, законодатель к настоящему времени лишь в уголовном законе (ст. 272 УК РФ) определил понятие компьютерной информации – это информация сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

На наш взгляд, компьютерная информация как предмет преступного посягательства – это совокупность фактических данных и команд, зафиксированных на машинном носителе или передающихся по телекоммуникационным каналам связи, предназначенных для использования в компьютере, компьютерной системе или сети, имеющим собственника, установившего правила пользования ими.

Исходя из изложенного, представляется целесообразным определить преступления в сфере компьютерной информации как противоправные виновно совершенные наказуемые в уголовном порядке общественно опасные деяния, посягающие на общественные отношения, обеспечивающие безопасность поиска, получения, передачи, производства, распространения компьютерной информации, применения информационных компьютерных технологий и их защиту, и причинившие вред, либо создавшие угрозу причинения вреда охраняемым законом правам и интересам физических и юридических лиц, общества, государства.

Итак, стремительное развитие компьютерных технологий и сетей, как неотъемлемой части современной телекоммуникационной системы, является одним из основных факторов, способствующих росту компьютерной преступности, которая становится одним из наиболее опасных видов преступных посягательств. Основным средством борьбы с преступлениями в данной сфере, на наш взгляд, должно быть уголовное законодательство, которое на протяжении последних 30 лет активно развивается как в зарубежных странах, так и в России.

1.2. Состояние, структура и динамика преступности в сфере компьютерной информации, тенденции ее развития

Компьютерная преступность появилась в нашей стране сравнительно недавно и в настоящее время является одним из самых «молодых» видов преступности. Несмотря на это данное явление все больше проявляет свою тенденцию к росту и является одним из наиболее вредоносных явлений современного мира. В доктрине информационной безопасности Российской Федерации одним из первоочередных мероприятий по реализации государственной политики обеспечения информационной безопасности РФ называется пресечение компьютерной преступности[51]. Выделение компьютерной преступности в структуре преступности позволяет детально изучить ее особенности и специфику, а также выработать эффективные меры борьбы с нею.

Преступность в сфере компьютерной информации, являясь разновидностью компьютерной преступности, представляет собой вид массового социально негативного общественно опасного поведения, запрещенного уголовным законом, складывающегося из противоправных посягательств на общественные отношения, обеспечивающие безопасность поиска, получения, передачи, производства, распространения компьютерной информации, применения информационных компьютерных технологий и их защиту, и причинившие вред, либо создавшие угрозу причинения вреда охраняемым законом правам и интересам физических и юридических лиц, общества, государства. Преступность, связанная с незаконным оборотом вредоносных компьютерных программ, является важной составной частью преступности в сфере компьютерной информации.

Последние десятилетия XX века ознаменовались беспрецедентным ростом компьютерной преступности, в том числе и преступности в сфере компьютерной информации, по всему миру, который затронул и Россию, где статистически это стало возможным наблюдать лишь с 1997 года, с принятием нового Уголовного кодекса. Высокая общественная опасность преступлений, совершаемых в сфере компьютерной информации, большое количество потерпевших, установленный и более значительный скрываемый материальный ущерб делают борьбу с этими негативными явлениями весьма актуальной. Уяснение сущности преступности в сфере компьютерной информации, выявление внутренних связей, зависимости от внешних факторов, определение основных тенденций и мер противодействия весьма условно без оценки статистического измерения данного феномена. В настоящее время, надо заметить, абсолютные цифры по данным ГИЦ МВД РФ невелики, а удельный вес в общем числе зарегистрированных преступлений составляет десятую долю процента, однако, обращают на себя внимание темпы роста преступности в сфере компьютерной информации – количество регистрируемых преступлений в сфере компьютерной информации представляет собой стабильно неуклонно растущую кривую, динамика роста которой превосходит практически любой из введенных в 1997

[51] Доктрина информационной безопасности РФ (утв. Президентом РФ 09.09.2000 № Пр-1895) // Российская газ. 2000. 28 сент. № 187.

году составов преступлений. Однако подобные цифры свидетельствуют не столько о росте количества совершаемых преступлений, сколько о снижении их латентности.

Среди качественных показателей преступности в первую очередь необходимо рассматривать ее структуру, причем критерии структуры преступности могут быть самыми разнообразными. Если иметь в виду преступность в сфере компьютерной информации, то в основе ее структуры, на наш взгляд, должен лежать уголовно-правовой признак.

Как свидетельствуют статистические данные, основу структуры преступности в сфере компьютерной информации в 1997-2012 годах составляют преступления связанные с неправомерным доступом к компьютерной информации (ст. 272 УК РФ) и созданием, использованием и распространением вредоносных программ для ЭВМ (ст. 273 УК РФ).

Изученные материалы судебной и следственной практики позволяют констатировать, что подавляющее большинство преступлений в сфере компьютерной информации совершается по корыстным мотивам (82%), среди иных побуждений можно выделить хулиганские побуждения, любопытство, месть, самоутверждение.

Преступления данного вида в 4 раза чаще совершаются мужчинами. Однако темпы роста женской преступности весьма велики из-за профессиональной ориентации некоторых специальностей и профессий. Интересно отметить, что по данным американских социологов женщины составляю треть от общего числа арестованных хакеров[52].

Возрастные характеристики компьютерных преступников выглядят следующим образом. До 2002 года подавляющее большинство выявленных лиц, совершивших преступления в сфере компьютерной информации, относились в возрастной категории от 25 до 35 лет. Начиная с 2003 года и по настоящее время большая часть злоумышленников – это молодые люди в возрасте от 18 до 25 лет. Похожие данные приводятся и в других исследованиях[53]. Например Осипенко А. Л. отмечает, что в настоящее время среди компьютерных преступников 20% составляют лица 14-18 лет, 57% - лица 19-25 лет, 15% - лица 26-35 лет, 8% - лица 36-55 лет[54]. Таким образом, в последнее время существует тенденция к омоложению компьютерных преступников, которая синхронизирует с общим омоложением преступности, и, в конечном счете может привести к тому, что в скором времени доля и общественная опасность хакеров, не достигших 16-летнего возраста, будет усиливаться по мере роста компьютеризации общества, хотя основная их часть будет состоять из лиц возрастной группы между 25-30 годами, как это имеет место в настоящее время в США[55].

Учитывая специфику объекта нашего исследования, хотелось бы отметить, что наибольший интерес для нас представляют преступления, связанные с созданием, использованием и распространением вредоносных компьютерных

---

[52] Кузнецов А. Пираты в Интернете // Милиция. 2000. № 2. С. 27.
[53] См.: Гаджиев М.С. Указ. соч. С. 47; Лопатина Т.М. Указ. соч. С. 264.
[54] Осипенко А.Л. Указ. соч. С. 164.
[55] Кузнецов А. Указ. соч. С. 27.

программ (ст. 273 УК РФ). Как свидетельствует уголовная статистика, научно-криминологические и иные информационно-аналитические данные период с 1997 по 2012 год характеризуется устойчивым ростом исследуемого вида преступности. Сложности, возникающие при расследовании дел данной категории, связаны, прежде всего, с трудностями выявления субъекта и места совершения преступления, а в случае установления субъекта и события преступления – с назначением и проведением экспертизы. До настоящего времени окончательно не сложилось однозначной терминологии, не созданы криминалистические экспертные лаборатории. Тем не менее, анализ судебной практики позволяет выделить основные группы преступных деяний, ответственность за которые предусмотрена статьей 273 УК РФ.

Во-первых, это распространение машинных носителей информации, содержащих вредоносные программы. Чаще всего такое распространение происходит путем продажи через розничную сеть компакт-дисков с коллекциями вредоносных программ. Статистика показывает, что наибольшее количество дел, квалифицированных по ст. 273 УК, составляют дела, в которых объективной стороной преступления является распространение вредоносных программ путем продажи лазерных компакт-дисков, содержащих такие программы.

Во-вторых, необходимо выделить распространение вредоносных программ через Интернет. Этот вид преступных деяний наиболее сложен для выявления и расследования, поскольку субъект и место совершения преступления могут находиться и за пределами России. Последствия же деяний могут характеризоваться огромным ущербом.

Третьим видом преступных деяний, квалифицируемых по признакам статьи 273 УК РФ, является модификация программистами работоспособных программ с целью блокирования или изменения их функций. Такие вредоносные программы, как правило, предназначены для достижения конкретных целей.

К четвертой группе преступных деяний, содержащих состав преступления по ст. 273 УК РФ, следует отнести создание и использование вредоносных программ – взломщиков паролей и программ-эмуляторов электронных ключей, которые применяются с целью незаконного использования или для создания контрафактных экземпляров программ для электронно-вычислительных машин и баз данных.

Рассматривая состояние преступности в сфере компьютерной информации, следует еще раз отметить, что во многом оно определяется тенденцией переноса центра тяжести на совершение подобных преступлений с использованием компьютерных сетей, и прежде всего Интернет. Число пользователей сети Интернет как во всем мире, так и в нашей стране постоянно растет. Если в 1999 году количество зарегистрированных пользователей в России составляло 1,5 млн человек, в 2002 году – 5,1 млн человек, то в 2005 году уже 22 млн человек. Каждый шестой россиянин, а в Москве – каждый второй, является пользователем Интернета. К 2008 году были подключены к глобальной сети все российские школы. В связи с уменьшающейся стоимостью и возрастающей миниатюризацией электронных компонентов сегодня самые современные технические средства стали доступными для широких слоев населения. Так, объем рынка инфор-

мационных технологий в России за 2010 год вырос на 23,6% и достиг 11 млрд. долл. Количество используемых персональных компьютеров в России превысило 17 млн единиц, увеличилось за 2010 год на 16%. Прогнозируется, что к 2013 году количество персональных компьютеров, используемых в бизнесе, возрастет в 6 раз; используемых населением – в 4 раза[56].

Расширение всемирной паутины и возрастание объема и качества доступных ресурсов сопровождается и соответствующим ростом различных злоупотреблений. Другими словами, статистический рост числа преступлений в сфере компьютерной информации коррелирует с ростом Интернета, причем пропорционально числу пользователей, что вполне объяснимо – состояние этого вида преступности напрямую зависит от общего уровня информатизации общества. Этот факт подтверждается результатами проведенного нами исследования. На вопрос анкеты о динамике роста количества преступлений в сфере компьютерной информации по мере компьютеризации российского общества, 98% опрошенных респондентов ответили: «Будет увеличиваться». По данным Интерпола Интернет стал той сферой, где «преступность растет самыми быстрыми темпами на планете». По данным Reuters, уже в 2004 году компьютерная преступность заработала 105 млрд. долларов, тем самым обойдя по официальной доходности наркоторговлю[57].

По прогнозам зарубежных экспертов ситуация с онлайновой преступностью будет все более усугубляться с каждым годом и начнет угрожать буквально каждому. По их мнению, основная угроза исходит из стран с неразвитой экономикой, в которых тем не менее имеются квалифицированные специалисты в области информационных технологий. В качестве примера можно привести 40 атак на коммерческие сайты, совершенные с территории стран бывшего Советского союза. По утверждению ФБР США, украденные хакерами номера кредитных карт, вероятно, в итоге попадают в руки местной организованной преступности[58].

Необходимо отметить, что компьютерные сети все шире применяются и во многих областях жизни и российского общества. Вместе с тем, растет количество преступлений, связанных с их использованием. За 2011 год Федеральная служба безопасности отразила свыше 1,4 миллиона интернет-атак на сайты федеральных органов государственной власти. Свыше 100 тысяч таких атак пришлось на официальное Интернет-представительство Президента России[59].

Интенсивное развитие российского сегмента Интернета, расширение системы электронной торговли, увеличение объемов финансовых операций с использованием компьютерных сетей, дает нам возможность прогнозировать рост данного вида преступлений. Таким образом, не исключено, что в скором времени проблема информационной безопасности станет в один ряд с такими гло-

---

[56] Дудинов А. Состояние и динамика развития Интернет в России в 2010 году [Электронный ресурс]// URL: http://webmastera.org/study/library.html?did=206.

[57] Мак-Клар С. Секреты хакеров. Безопасность сетей - готовые решения / С. Мак-Клар, Д. Скембрей, Д. Курц [Электронный ресурс] // URL: http://data.mf.grsu.by/citforum/htdocs/book/hacker2sek/hacker2sek_vv.shtml.

[58] См.: Старостина Е.В. Защита от компьютерных преступлений и кибертерроризма / Е.В. Старостина, Д.Б. Фролов. М.: Изд-во Эксмо, 2005. С. 90.

[59] ФСБ отразила 1 млн компьютерных атак. Вебпланета [Электронный ресурс] // URL: http://www.webplanet.ru/news/lenta/2005/12/16/fsbb.html.

бальными проблемами современности, как экологический кризис, организованная преступность, коррупция, отсталость развивающихся стран и др. Данные обстоятельства заставляют вырабатывать новые подходы к защите интересов личности, общества и государства в этой сфере.

Осмысление сущности глобальных компьютерных сетей позволяет заключить, что в целом не является преувеличением отношение отдельных авторов к этому явлению как к некому феномену, в определенной степени оказывающему непосредственное влияние на структуру современной преступности, в качестве специфических свойств которого называются:

- технологическая незащищенность глобальных сетей,
- возможность анонимной деятельности в глобальных сетях,
- сложность инфраструктуры современных сетей и сетевых процессов,
- влияние глобальных компьютерных сетей на состояние национальной безопасности,
- отсутствие единой организации полностью координирующей деятельность Интернета,
- надгосударственный характер современных глобальных сетей[60].

Значительную опасность представляет так же та распространенность, которую за последние 40 лет приобрело такое явление, как создание вредоносных компьютерных программ, особенно вирусных. Одно из недавних исследований установило, что новый компьютер, только что подключенный к Интернету и не имеющий антивирусной программы, будет заражен в течение 20 минут[61].

Однажды Интернет погибнет от компьютерных вирусов, заявила британская компания MassageLabs, по их мнению, в сети просто невозможно будет работать из-за постоянных вирусных эпидемий. Еще в 1987 г. специалисты доказали невозможность разработки алгоритма, способного обнаруживать все возможные вирусы. Более того, исследования компании IBM показали, что возможно создание вирусов, выявление которых будет затруднено даже при наличии образца вируса. Иными словами, нет и не может быть программ, определяющих все известные вирусы[62].

Достаточно сложно оценить наносимый вирусами ущерб, поскольку при этом необходимо проанализировать массу показателей, трудно поддающихся учету. Основные издержки связаны с простоями вычислительных систем, очисткой их от зараженных файлов, восстановлением информации, внедрением нового защитного программного обеспечения, ухудшением репутации пострадавших фирм. Приводимые различными компаниями данные существенно отличаются друг от друга. Тем не менее их анализ показывает, что ущерб, наносимый при распространении вирусов по компьютерным сетям огромен и растет с каждым годом (так в 2005 году ущерб составил 11 млрд. долл., в 2006 г. – 12,5 млрд. долл., в 2007 г. – 18 млрд. долл., в 2008 г. – 14 млрд. долл., в 2009 г. – 16

---

[60] См.: Осипенко А.Л. Указ. соч. С. 38-56.

[61] Руководство пользователя по обеспечению безопасности при работе на компьютере. Информационные технологии и электронные коммуникации [Электронный ресурс] // URL: http://www.itaec.ru/Information/secrt.html.

[62] См.: Осипенко А.Л. Указ. соч. С. 85.

млрд. долл., в 2010 г. – 20 млрд. долл.[63]). А так как, по результатам проведенного нами исследования количество преступлений в сфере компьютерной информации и преступлений, связанных с незаконным оборотом вредоносных компьютерных программ, будет увеличиваться, то можно прогнозировать и рост материального ущерба от преступлений данного вида.

Нельзя не согласиться с некоторыми исследователями, которые сравнивают вредоносные программы с информационным оружием, которому свойственны универсальность, радикальность воздействия, доступность, широкие возможности места и времени применения, высокая эффективность на значительных расстояниях, скрытность использования[64].

С 2005 года специалистами констатировалось двойное увеличение количества вредоносных программ, которые все чаще создаются не хакерами-самоучками, а организованными преступными группами с целью извлечения коммерческой выгоды. Как результат, число вирусных эпидемий уменьшилось, они стали локальными, целенаправленными. Неоднократно говорилось о растущей изощренности атак. От грубых методов злоумышленники переходят к точечным атакам на интересующие их организации и людей, к поиску и использованию уязвимостей в программном обеспечении[65].

Преступность в сфере компьютерной информации в целом и преступность, связанная с незаконным оборотом вредоносных компьютерных программ, в частности имеет характерные черты, рассмотреть которые нам представляется целесообразным.

Во-первых, данный вид преступности характеризуется очень высоким уровнем латентности. Так, по данным Национального отделения ФБР по компьютерным преступлениям от 85 до 97% компьютерных посягательств даже не выявляются[66]. По оценкам иных экспертов, латентность «компьютерных» преступлений в США достигает 80%, в Великобритании — до 85%, в ФРГ — 75%, в России — более 90%. За рубежом, где накоплена достаточно большая и достоверная статистика подобных преступлений, до суда доходят меньше 1% нарушений[67].

В 2008 году Институтом защиты компьютеров США совместно с ФБР было проведено исследование, направленное на определение распространенности таких преступлений и мер, принимаемых для их предотвращения. Ответы были получены из 428 организаций.

Респонденты подтвердили, что их информационные системы находятся в опасности. 42% испытали некоторою форму вторжения или другого несанк-

---

[63] Угрозы информационной безопасности. Лаборатория Касперского [Электронный ресурс] // URL: http://www.kaspersky.ru/corporatesolutions.

[64] См.: Крутских А.В. Информационный вызов безопасности на рубеже XXI века // Международная жизнь. 1999. №2. С. 82 – 89.

[65] Руководство пользователя по обеспечению безопасности при работе на компьютере. Информационные технологии и электронные коммуникации [Электронный ресурс] // URL: http://www.itaec.ru/Information/secrt.html .

[66] Айков Д. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями / Д. Айков, К. Сейгер, У. Фонсторх; Перевод с английского. М.: Мир, 1999. С.5.

[67] Сабадаш В. Компьютерные преступления: 15 раскрыто, 85 – в тени [Электронный ресурс] // URL: http://www.hackzona.ru/hz.php?name=News&file=article&sid=2977.

ционированного использования компьютерных систем в течение последних 12 месяцев.

Свыше 50% из тех, кто испытал вторжение или делал попытку исследований собственных информационных систем, установили факты несанкционированных действий со стороны собственных служащих. Несанкционированное вторжение в информационные системы были также распространены из удаленных источников и сети Интернет. Что касается частоты вторжений, то 22 респондента указали, что они испытали 10 или большее количество «нападений» на их системы в течение прошедшего года.

Опрос также показал следующее:

Свыше 50% ответивших не имеют плана действий на случай сетевого вторжения.

Свыше 60% - не имеют стратегии сохранения доказательств для дальнейшего судебного рассмотрения уголовных или гражданских дел.

Свыше 70% респондентов не имеют устройств, предупреждающих о вторжении в их коммуникационные и информационные системы.

Менее 17% указали, что они уведомят правоохранительные органы в случаях нападения на информационные системы.

Свыше 70 % назвали в качестве основной причины отказа обращаться в правоохранительные органы опасение антирекламы[68].

Надо заметить, что степень латентности преступлений, связанных с незаконным оборотом вредоносных программ, еще более высока. По мнению экспертов, технически невозможно в 999 из 1000 случаев поймать преступника, так как ежедневно десятки вирусов запускаются в сеть Интернет от разных авторов и со всех концов света, без видимых признаков идентификации производителя[69].

По-латински latens (latentis) – скрытый, внешне не проявляющийся. Латентной частью преступности, или иногда латентной преступностью, называют то множество преступлений, которое не отражено в статистике[70]. Одна из важных задач изучения преступности – это выявление не статистической картины преступности, а преступности фактической.

В структуре латентной преступности по механизму ее образования выделяют четыре разновидности[71].

К естественно-латентным следует относить совокупность преступлений, не ставших достоянием органов и учреждений, регистрирующих их и осуществляющих преследование виновных, соответственно не учтенных в уголовной статистике, и в отношении которых не приняты предусмотренные законом меры реагирования. В зависимости от специфики факторов, способствующих естественной латентности преступлений, они, в свою очередь, могут быть подразделены на четыре группы.

---

[68] Мак-Клар С. Указ. соч.

[69] Там же.

[70] Криминология / Под общ. ред. А.И. Долговой. М.: Норма, 2005. С. 92.

[71] См.: Акутаев Р.М. Криминологический анализ латентной преступности: Автореф… дис. д-ра юрид. наук. СПб, 1999.

Первая группа включает преступления, о совершении которых может не знать никто, включая и самого правонарушителя. Это – преступления, совершенные по небрежности, либо ситуации, когда в силу правовой некомпетентности участники правоотношений допускают подмену одной нормы (уголовно-правовой) другой (нравственной или административной).

Ко второй группе можно отнести преступления, где потерпевшие не сообщают о них в силу незаинтересованности в их выявлении. Мотивы такой незаинтересованности могут быть различными. Иногда руководители опасаются подрыва своего авторитета в деловых кругах и в результате – потери большого числа клиентов, раскрытия в ходе судебного разбирательства системы безопасности организации, выявления собственной незаконной деятельности. Также необходимо отметить, что многие организации разрешают конфликт своими силами, поскольку убытки от расследования могут оказаться выше суммы причиненного ущерба (изъятие файлового сервера для проведения экспертизы может привести к остановке работы на длительный срок, что неприемлемо ни для одной организации). Среди иных причин можно назвать отсутствие уверенности потерпевшей стороны в наказании виновных, возврате потерянных денежных средств и т.д. Кроме того, одной из причин латентности является слабый уровень правосознания населения, незнание своих прав и нежелание добиваться защиты своих прав и законных интересов правовыми методами.

Третью группу составляют преступления, где нет явно выраженной потерпевшей стороны, поэтому и некому сообщить о преступлении в компетентные органы. Нередко такое можно встретить при посягательствах на государственные или общественные интересы.

Четвертая группа - преступления, где факт его совершения известен узкому кругу лиц либо только виновному лицу. Это касается, например, такого способа преступной деятельности в сфере компьютерных технологий, как неправомерный доступ к компьютерной информации с целью получения возможностей знакомиться и осуществлять операции с чужой информацией, находящейся в ЭВМ и на машинных носителях, т.е. действия, направленные прежде всего на нарушение конфиденциальности информации. Неправомерный доступ к компьютерной информации может включать в себя: хищение и (или) копирование, подмену машинных носителей информации; копирование документов с исходными данными и выходных документов; использование визуальных, оптических и акустических средств наблюдения за ЭВМ; считывание и расшифровку различных электромагнитных излучений в ЭВМ и в обеспечивающих системах; запоминание информации; фотографирование информации в процессе ее обработки; изготовление дубликатов входных и выходных документов; копирование распечаток и т.д. Очень часто в таких случаях потерпевшие даже не догадываются о преступных действиях, совершенных против них и направленных на нарушение конфиденциальности информации, так как в отличие от бумажных носителей информация никуда не исчезает. В итоге о преступном посягательстве знают только преступники, и эта часть преступлений является латентной.

Вторую разновидность латентной преступности – совокупность искусственно латентных преступлений – образуют как известные правоохранительным органам преступления, но не взятые ими на учет, так и учтенные, но не раскрытые либо неполно раскрытые. Искусственно латентные преступления могут быть представлены в двух группах.

Первая группа включает неучтенные правоохранительными органами преступления, по которым уголовные дела не возбуждены, хотя информацией о них располагают те или иные учреждения, предприятия, организации, она стала достоянием и правоохранительных органов, но последние не принимают необходимых мер к законной реализации этой информации. Такие действия могут осуществляться, например, с той целью, чтобы путем манипуляций со статистикой создать видимость уголовного благополучия в районе, городе, области; иногда это незаконное сокрытие совершенных преступлений с корыстной целью или вследствие иной личной заинтересованности.

Вторую группу составляют субъектно-латентные преступления. Это – нераскрытые (неполно раскрытые) преступления, когда сам факт их известен и учтен, но неизвестно и не привлечено к уголовной ответственности лицо, совершившее преступление, или отдельные из них, если преступление совершено в соучастии. Субъектно-латентные преступления отличаются от иных форм проявления латентности главным образом тем, что в данном случае речь идет о латентности субъекта, совершившего уголовно-противоправное деяние, а не латентности преступления. В подобных ситуациях лицо, виновное в совершении преступления, по причине его неустановленности не претерпевает тех неблагоприятных для него последствий, которые предусмотрены уголовным законом. Безнаказанность также ведет к игнорированию, а в конечном счете и подрыву принципа неотвратимости уголовной ответственности и принципа равенства граждан перед законом, закрепленного ст. 4 УК РФ как одного из важных отправных начал российского уголовного права.

Третью разновидность латентной преступности иногда определяют термином «пограничные ситуации». Она представляет собой группу тех преступлений, информация о которых стала известна правоохранительным органам, но их конкретный работник, ошибочно, добросовестно ошибаясь или не имея достаточной профессиональной подготовки, дал неправильную юридическую оценку деянию, не увидев в нем признаков состава преступления, в связи с чем оно оказалось за статистическим учетом.

Не взвешенная политика государства по сокращению штатов правоохранительных органов, низкий уровень материального и финансового обеспечения влекут за собой отток высококвалифицированных кадров. Кроме того, правоохранительные органы не могут обеспечить соответствующую реакцию на постоянно возрастающий объем оперативной информации о преступлениях в сфере компьютерной информации, которую они должны в полном объеме обработать. Чем больше ресурсные ограничения, тем больший объем сигналов о преступлениях система правоохранительных органов вынуждена от себя оттолкнуть, оставляя их в «латентной тени». Исследования различных стран на уровне статистической закономерности свидетельствуют о том, что рост преступности на 2-3 % вызывает сни-

жение раскрытия преступлений на 1 %, что, в свою очередь, увеличивает количество уклонения правонарушителей от ответственности.

В научном и практическом плане представляет определенный интерес и понятие мнимой латентности, под которым следует понимать ошибочное восприятие деяния как преступного, оставшегося без соответствующего реагирования со стороны компетентных органов. Проявлением мнимой латентности являются случаи, когда лица, считающие себя потерпевшими от преступления, заявляют об этом в официальные органы, хотя по критериям уголовного права деяние «виновного» лица не содержит состава преступления.

Как видим, понятия «пограничные ситуации» и мнимая латентность хотя и близки по содержанию, но не совпадают. Основное их отличие состоит в характере субъективного восприятия деяния, от чего во многом зависит выбор дальнейшего поведения лица, в частности, заявить о случившемся в правоохранительные органы или нет.

Помимо указанных причин, некоторые авторы отмечают и другие причины латентности преступности в сфере компьютерной информации. Так, например, С.Г. Спирина связывает латентность таких преступлений с:

а) нежеланием потерпевших делать заявления в органы милиции;

б) неопытностью правоохранительных органов в расследовании этих преступлений;

в) трудностями квалификации;

г) отсутствием специализированных экспертиз для расследования таких преступлений;

д) трудностями при доказательствах;

е) компьютерной неграмотностью и отсутствием компьютерной культуры[72].

Иногда высказывается мнение, что без латентности преступности система борьбы с преступностью буквально рухнула бы под тяжестью последней, будучи не в состоянии «перерабатывать» все данные о ней. Действительно, существующая система с ее численностью сотрудников и кадровым составом не способна к такой полной «переработке». Однако выход состоит не в том, чтобы смириться с латентностью преступности, а в совершенствовании самой борьбы[73].

Исследуя статистические данные о показателях преступности в сфере компьютерной информации, мы видим, что эти сведения представляют собой показатели борьбы с подобной преступностью следственно-судебных органов, таким образом, статистика лишь в самой малой мере отражает уровень деяний и чуть больше их общие тенденции[74]. Вместе с тем совсем игнорировать данные официальной статистики нельзя, так как они все же имеют достаточно серьезное научное значение, поскольку в определенной степени отражают состояние, интенсивность, возможности того или иного направления уголовной политики, указывая на цели и пути ее совершенствования при необходимой критичности

---

[72] Спирина С.Г. Криминологические и уголовно-правовые проблемы преступности в сфере компьютерной информации: Дис. … канд. юрид. наук. Краснодар, 2001. С. 36-37.

[73] Криминология / Под общ. ред. А.И. Долговой. М.: Норма, 2005. С. 130.

[74] См.: Лунеев В.В. Преступность XX века. М., 1997.

и взвешенности в их оценках. Но при изучении уголовной, судебной статистики всегда должна ставиться задача определить степень латентной преступности.

Латентность бывает особенно высокой при наличии развитой организованной и профессиональной криминальной деятельности. К числу важных характеристик последней относятся: создание специальной системы самозащиты от обнаружения, разоблачения и привлечения виновных к установленной законом ответственности; особенно тщательная маскировка преступлений; максимальное придание им видимости легальной деятельности – соответствующей правовым нормам, закону.

Преступность в сфере компьютерной информации и особенно та ее разновидность, которая связана с незаконным оборотом вредоносных компьютерных программ, обладает признаками профессиональной преступности, среди которых можно выделить следующие:

1) устойчивый вид занятий, наличие определенных специальных и знаний и навыков, необходимых для занятия преступной деятельностью;

2) определенная криминальная специализация этих лиц, совершение преимущественно однородных преступлений;

3) преступная деятельность для этих лиц является основным, а иногда и единственным источником дохода;

4) связь с асоциальной средой[75].

Поскольку криминальный профессионализм включает и овладение способами маскировки преступлений, нередко преступники, владеющие соответствующими навыками, совершают серию преступлений, многоэпизодные преступления, не будучи выявленными. Такие преступления часто не раскрываются, и профессиональные преступники не оказываются среди рецидивистов.

Преступность в сфере компьютерной информации носит организованный и транснациональный характер. По мнению специалистов около 62% компьютерных преступлений совершается в составе организованных групп, в том числе и на территории нескольких стран[76]. Этот факт подтверждается и данными проведенного нами исследования. Так, на вопрос анкеты «Считаете ли Вы, что преступность в сфере компьютерной информации в России носит организованный транснациональный характер?», 82% опрошенных респондентов дали положительный ответ. Однако, по данным ГИЦ МВД РФ, при 10191 зарегистрированному в 2007 году преступлению, было выявлено лишь 19 организованных групп их совершающих, в 2008 году при 8889 зарегистрированных преступлениях, выявлено 18 организованных групп, в 2009 году при 7236 зарегистрированных преступлениях, выявлено 203 организованных группы. Такая статистика, на наш взгляд, свидетельствует о значительных трудностях, с которыми сталкиваются правоохранительные органы при выявлении подобных групп. Однако, с другой стороны она показывает значительный рост подобных преступлений, совершенных организованными группами или преступными сообществами.

---

[75] См.: Гуров А. И. Профессиональная преступность. М., 1990.

[76] Криминология / Под общ. ред. А.И. Долговой. М.: Норма, 2005. С. 744.

Транснациональная организованная преступность – наиболее рациональная и профессиональная часть криминального поведения, создающая прямую угрозу национальной и международной безопасности и стабильности. Трансграничные преступления в сфере компьютерной информации затрагивают интересы граждан или юридических лиц других стран, совершаются в рамках «всемирной паутины» - пространстве, в котором отсутствуют географические и геополитические границы государств и не действует их юрисдикция. Глобализация компьютерных сетей обусловливает несоизмеримо широкий круг участников, разнообразие каналов передачи данных, программного и аппаратного обеспечения, многообразие и недостаточную правовую регламентацию возникающих ситуаций.

Попытки собрать мировую статистику об организованной преступности предпринимают Интерпол, ООН и другие международные организации. Несмотря на это уровень контроля над деятельностью транснациональной организованной преступности остается достаточно слабым.

Рентабельность криминального бизнеса с использованием компьютерных технологий весьма велика, что стимулирует объединение хакеров в преступные группы, складывание вокруг них криминальной среды. По прогнозам экспертов, повсеместная разработка и применение современных технологий наряду с плохо оснащенными органами компьютерной безопасности неизбежно приведут к созданию глобальной организованной сети киберпреступников. Действительно, все чаще на лентах Интернет-агентств появляются сообщения о хакерских атаках. К примеру, на официальный сайт ФСБ России в 2007 году было совершено около 600 подобных нападений. По данным американского ФБР, за несколько месяцев 2008 года был раскрыт ряд организованных групп хакеров из Восточной Европы, прежде всего из России и Украины[77].

Известное преступление В. Левина и других отнесено к категории «транснациональных сетевых компьютерных преступлений», совершаемых преступными международными организациями. В организацию входило 12 человек, из них 10 граждан России и 2 гражданина Нидерландов. Одни из членов преступной группы осуществляли неправомерный доступ к компьютерной информации, другие снимали похищенные деньги и осуществляли их транспортировку. В частности, в период с июня по октябрь 1994 г. в Санкт-Петербурге из офиса АО «Сатурн», принадлежавшего Владимиру Левину и Алексею Галахову, совершались действия по неправомерному доступу в систему управления денежными операциями «Ситибанка» (г. Нью-Йорк, США). Эта система использовалась для расчетов между финансовыми организациями, расположенными по всему миру. Финансовые операции инициировались клиентами при помощи доступа по телефонным каналам связи или с использованием сети передачи данных «Спринт/Теленет». Зная пароли и идентификаторы пользователей, используемые в системе управления денежными операциями «Сити-банка», преступники пытались осуществить сорок переводов на сумму около 10 млн долларов США. Реально им удалось незаконно перевести 400 тыс. долларов. Счета пострадавших находились в США, Канаде, Ар-

[77] Россия в фокусе криминальной глобализации. Владивостокский центр исследования организованной преступности [Электронный ресурс] // URL: http://www.crime.vl.ru/index.php?p=1382&more=1&page=2.

гентине, Новой Зеландии, Колумбии, Гонконге, Индонезии и Уругвае. Переводились похищенные деньги в США, Россию, Финляндию, Нидерланды, Германию, Швейцарию и Израиль[78].

К особенностям исследуемого вида преступности следует отнести также то, что данный вид преступности характеризуется постоянным наращиванием и совершенствованием способов совершения преступлений[79]. Так, в кодификатор компьютерных преступлений Генерального Секретариата Интерпола включено около семи способов компьютерного мошенничества, четырех способов незаконного копирования, пяти способов изменения компьютерных данных, трех способов компьютерного саботажа. Представленные виды преступлений и их характеристики формировались на протяжении тридцати с лишним лет. На сегодняшний день техническая культура стала носить массовый характер, а технические знания находить массовое применение. Мы уже не акцентируем внимание на компьютерном шпионаже, вымогательстве, мошенничестве и саботаже. Сегодня мир беспокоят информационный терроризм, информационные войны, деятельность компьютерной мафии, транснациональный и организованный характер преступлений, совершаемых с использованием высоких технологий.

Таким образом, проведенный анализ преступности связанной с незаконным оборотом вредоносных компьютерных программ и ее проявлений на современном этапе позволяет выявить следующие тенденции в ее развитии: продолжение процесса устойчивого роста количества таких преступлений, и как следствие, увеличение материального ущерба, ими причиняемого; перенос центра тяжести на совершение подобных преступлений с использованием компьютерных сетей, и прежде всего Интернет; омоложение компьютерных преступников. Данный вид преступности характеризуется: высоким уровнем латентности; корыстной мотивацией; международным и организованным характером, наличием признаков профессиональной преступности, постоянным совершенствованием способов совершения преступлений для обеспечения безопасности незаконной деятельности.

---

[78] См.: Овчинский А.С. Анализ опыта использования современных информационных технологий преступными группировками; хакерские технологии в сети Интернет / А.С. Овчинский, И.А. Наумов // Хакеры против банков: Консультационно-информационный семинар. М., 1998. С. 12-13.

[79] Криминология / Под общ. ред. А.И. Долговой. М.: Норма, 2005. С. 745.

УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ НЕЗАКОННОГО ОБОРОТА ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ

2.1. Вредоносная компьютерная программа: понятие и виды

Как мы уже отмечали в п. 1.1, предметом преступного посягательства преступлений в сфере компьютерной информации является компьютерная информация. При этом возникает вопрос о соотношении понятий «компьютерная информация» и «вредоносная компьютерная программа». Компьютерная программа фактически имеет двойственную природу[80]: с одной стороны, она может являться инструментом воздействия на компьютерную информацию, с другой – она сама как компьютерная информация в виде совокупности команд и данных является предметом преступного посягательства (ст. 273 УК). Поэтому вредоносную компьютерную программу следует рассматривать как разновидность компьютерной информации, содержащей определенные сведения, компилированные в читаемый набор машинных символов.

В законодательстве[81] под термином «вредоносная компьютерная программа», понимается программа, заведомо предназначенная для несанкционированного уничтожения, блокирования, модификации либо копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

В технической литературе чаще используются другие термины: «информационная инфекция», «логическая инфекция», «разрушающее программное воздействие», «программы с потенциально опасными последствиями» и другие. Иногда для обозначения всех вредоносных программ, а не только их отдельного класса, используются термины «компьютерный вирус», «вирус», «закладка», «программная закладка», «троянская программа»[82].

В технической литературе дается большое количество различных определений вредоносным компьютерных программам, однако упор в них делается на основные функциональные характеристики[83].

В юридической литературе также дается несколько определений вредоносных программ, но следует обратить внимание, что некоторые авторы отождествляют это понятие с понятием компьютерного вируса[84]. Так, по мнению В.В. Крылова, вредоносной является специально разработанная или моди-

---

[80] См.: Лопатина Т.М. Указ. соч. С. 206.

[81] См. ст. 273 УК РФ; ст. 1 Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (Минск, 01.06.2001).

[82] Соловьев Л.Н. Вредоносные программы: расследование и предупреждение преступлений. М.: Собрание, 2004. С. 16.

[83] См.: Ярочкин В.И. Безопасность информационных систем. М.: «Ось-89», 1996. С. 124; Белкин П.Ю. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учебное пособие для вузов / П.Ю. Белкин, О.О. Михальский, А.С. Першаков и др. М.: Радио и связь, 1992. С. 133-134.

[84] См.: Гульбин Ю. Преступления в сфере компьютерной информации // Российская юстиция. 1997. № 10. С. 25; Ваулина Т.Н. Преступления в сфере компьютерной информации / Уголовное право. Особенная часть // Отв. ред. И.Я. Козаченко и др. М.: ИНФРА-М-НОРМА, 1997. С. 559; Никулин С.И. Преступления в сфере компьютерной информации / Уголовное право. Особенная часть: Учебник // Под ред. А.И. Рарога. М.: Триада, Лтд, 1996. С. 325; Старостина Е.В. Указ. соч. С. 16.

фицированная программа для несанкционированного собственником информационной системы уничтожения, блокирования, модификации либо копирования информации, нарушения обычной работы ЭВМ. При этом под вредоносной программой Крылов понимает «компьютерный вирус»[85].

С.В. Полубинская и С.В. Бородулин в учебнике «Российское уголовное право. Особенная часть» указывают, что в ст. 273 УК РФ речь идет о разработке и распространении так называемых компьютерных вирусов, как путем создания подобных программ, так и путем внесения изменений в уже существующие программы[86].

Однако, на наш взгляд, с данным подходом нельзя согласиться. Представляется, что все многообразие вредоносных программ только лишь компьютерными вирусами не ограничивается. Особенностью вирусов является его способность самовоспроизводиться, размножаться, присоединяться к другим программам. К вредоносным программам, помимо компьютерных вирусов, относятся также программы, не способные к самораспространению (например, программные закладки), которые в остальном могут быть наделены аналогичными с самораспространяющимися программами функциями. Употребление в качестве синонимов таких понятий как «вредоносная» и «вирусная» программа ведет к неоправданному сужению признаков объективной стороны рассматриваемого преступления, что создает возможность для безнаказанности за незаконный оборот вредоносных компьютерных программ, не являющихся по своим качественным характеристикам вирусными. Таким образом, понятие «вредоносная программа» является родовым по отношению к понятию «компьютерный вирус». С этим очевидно согласен законодатель, заменив в проекте уголовного кодекса термин «компьютерный вирус», как предмет преступления, связанного с незаконным оборотом вредоносных компьютерных программ, на термин «вредоносная компьютерная программа», дав тем самым возможность расширенно толковать данное понятие.

Все вредоносные программы обладают некоторыми особенностями, позволяющими выделить их в отдельный класс программ:

1) способностью совершать действия, приводящие к уничтожению, блокированию, модификации либо копированию информации, нейтрализации средств защиты компьютерной информации;

2) несанкционированность данных действий владельцем или пользователем информации.

Уничтожение информации – удаление информации, находящейся на любом машинном носителе, и невозможность ее восстановления на нем.

Перевод информации на другой машинный носитель не считается в контексте уголовного закона уничтожением компьютерной информации лишь в том случае, если в результате этих действий доступ правомерных пользователей

---

[85] См.: Крылов В.В. Информационные компьютерные преступления. М.: Издательская группа ИНФА-М-НОРМА, 1997. С. 41-42.

[86] См.: Бородин С.В. Преступления в сфере компьютерной информации / Российское уголовное право. Особенная часть / С.В. Бородин, С.В. Полубинская; Под ред. В.Н. Кудрявцева, А.В. Наумова. М.: Юристъ, 1997. С. 350.

к информации не оказался существенно затруднен либо исключен. Уничтожением информации не является переименование файла, где она содержится, а также, само по себе, автоматическое «вытеснение» старых версий файлов последними по времени.

Блокирование информации - совершение действий, приводящих к ограничению или закрытию доступа к компьютерной системе и предоставляемым ею информационным ресурсам, искусственное затруднение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением.

Модификации информации – любое ее изменение, в том числе и перевод с одного языка на другой, за исключением адаптации, то есть внесения изменений, осуществляемых исключительно в целях функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя (ст. 1270 ч. 4 ГК РФ)[87].

Копирование информации – перенос информации на другой обособленный от компьютера носитель при сохранении неизменной первоначальной информации, воспроизведение информации в любой материальной форме: от руки, путем фотографирования текста с экрана дисплея, а также считывания информации путем перехвата излучений компьютера и т.д.

От копирования компьютерной информации следует отличать размножение информации. В последнем случае информация повторяется не на обособленном от оригинального носителе, а на оригинальном носителе (например, в дисковой памяти компьютера организуются несколько файлов одного и того же содержания) либо на однородном носителе, оставшемся в распоряжении пользователя (например, копия располагается в дисковой памяти, образующей с данным компьютером систему, либо на дискете, сознательно оставленной в компьютере).

Перечисленные выше последствия являются основными разновидностями ущерба, причиняемого информации в результате воздействия на неё вредоносных компьютерных программ. Что касается такого последствия воздействия вредоносных программ как «нейтрализация средств защиты компьютерной информации», то на наш взгляд данное последствие является производным от перечисленных четырёх способов нарушения порядка использования компьютерной информации. Нейтрализация средств защиты компьютерной информации может явиться следствием поражения компьютерной информации, в результате чего происходит нарушение работы как отдельных программ, баз данных, выдача искаженной информации, так и нештатное функционирование аппаратных средств и периферийных устройств, либо нарушение нормального функционирования сети, в том числе прекращение функционирования автоматизированной информационной системы в установленном режиме, либо сбой в обработке компьютерной информации.

Термин «несанкционированные действия» подразумевает отсутствие разрешения, которое должен дать собственник (владелец) информационного ресурса.

---

[87] См.: Собрание законодательства РФ. 2006. № 52 (1ч.). Ст. 5496; 2007. № 49. Ст. 6079.

Иными словами, вредоносность компьютерной программы определяется не ее назначением и способностью уничтожать, блокировать, модифицировать, копировать информацию (это вполне типичные функции легальных программ), а тем, предполагает ли ее действие, во-первых, предварительное уведомление собственника компьютерной информации или другого добросовестного пользователя о характере действия программы, а, во-вторых, получение его согласия (санкции) на реализацию программой своего назначения. Нарушение одного из этих требований делает компьютерную программу вредоносной.

Таким образом, вредоносную программу можно определить как компьютерную программу, функционирование которой вызывает несанкционированное собственником компьютерной информации ее уничтожение, блокирование, модификацию либо копирование.

Все вредоносные программы могут быть классифицированы по различным основаниям. Вредоносные программы в зависимости от наличия в них открыто декларируемых функций можно разделить на: троянские программы и скрытые вредоносные программы[88].

В литературе термин троянская программа иногда используется для обозначения всех вредоносных программ, иногда только какого-то вида вредоносных программ. В данном случае под троянской программой понимается программа, которая, помимо полезных и нужных функций, втайне от пользователя выполняет некоторые другие функции, заложенные в ее алгоритм создателем, с целью причинения пользователю определенного ущерба[89].

Отличием скрытых вредоносных программ является то обстоятельство, что о наличии, запуске и функционировании скрытой вредоносной программы пользователю не известно.

К троянским программам относятся в основном программные закладки, к скрытым вредоносным программам могут относиться программы всех групп: компьютерные вирусы, компьютерные черви, программные закладки.

Анализ специальной научной литературы[90] дает нам основание классифицировать все вредоносные программы по объекту воздействия на:

- программы, влияющие на аппаратно-техническую часть средств компьютерной техники (повреждающие микросхемы, диски, принтеры, выжигающие люминофор);

- программы, влияющие на программную составляющую средств компьютерной техники (повреждающие системную информацию: области диска, форматирующие носители, файлы информационной системы);

- программы, влияющие на компьютерную информацию (нарушающие конфиденциальность информации (свойство информации быть известной только определенному кругу лиц); целостность информации (состояние данных при

---

[88] См.: Соловьев Л.Н. Указ. соч. С. 35-36.

[89] Сырков Б. Троянские программы / Системы безопасности, связи и телекоммуникации. 1999. № 30. С. 66.

[90] См. подробнее: Фролов А.В. Осторожно: компьютерные вирусы / А.В. Фролов, Г.В. Фролов. М.: ДИАЛОГ-МИФИ, 1996; Файтс Ф. Компьютерный вирус: проблемы и прогноз: Пер. с англ. / Ф. Файтс, П. Джонстон, М. Кратц. М.: Мир, 1994; Безруков Н.Н. Классификация компьютерных вирусов MS DOS и методы защиты от них. М.: СП «ICE», 1990; Соловьев Л. Н. Вредоносные программы: расследование и предупреждение преступлений. М.: Собрание, 2004.

котором они сохраняют свое информационное содержание и однозначность интерпретации в условиях случайных воздействий); доступность информации (свойство информации быть доступной для пользователя в любое время).

- программы, влияющие на пользователя компьютера (воздействующие на зрение, психику и др. В литературе описан случай инициирования мерцания монитора компьютера с определенной периодичностью, способной вызвать эпилептические припадки. Отмечается, что подобные программы могут быть использованы также для ввода сообщений на уровне подсознания[91]. Также, появлялись сообщения о компьютерном вирусе «666», который, выводя каждую секунду на монитор 25-й кадр, вызывал у пользователя кровоизлияние в мозг и смерть[92]. Однако, официально зарегистрированных фактов такого воздействия пока выявлено не было.)

По своим деструктивным возможностям все вредоносные программы можно разделить на[93]:

- условно-безвредные, не влияющие на работу компьютерной системы, кроме уменьшения количества свободной памяти;

- неопасные, влияние которых ограничивается уменьшением свободной памяти на диске, а также графическими, звуковыми и прочими эффектами;

- опасные, которые могут привести к серьезным сбоям в работе компьютерных систем;

- очень опасные, которые могут привести к потере программ, уничтожению данных, стиранию информации в системных областях памяти, способствовать быстрому износу движущихся частей механизмов и даже преждевременному выходу из строя периферийных устройств.

Однако, на наш взгляд, безвредность вредоносных программ является достаточно относительным понятием и ему трудно найти уголовно-правовое или криминологическое применение. Любая вредоносная программа может, во-первых, содержать ошибки, во-вторых, она может проявлять новые качества в новых условиях работы (например, при работе с новой операционной системой), в-третьих, она всегда нарушает авторское право или право собственника на информацию, в-четвертых, она с легкостью может быть переделана в опасные и особо опасные разновидности программ. Поэтому нельзя согласиться с мнением В.Ю. Максимова, который считает, что наибольшее значение для уголовного права представляет классификация вредоносных программ по деструктивным возможностям, и предлагает решить вопрос об ограничении незаконного обращения с безвредными программами в рамках не уголовного, а административного права[94].

В зависимости от наличия функции самораспространения вредоносные программы делятся на самораспространяющиеся программы и программы не способные к самораспространению. Функция самораспространения заключает-

---

[91] Курушин В.Д. Компьютерные преступления и информационная безопасность / В.Д. Курушин, В.А. Минаев. М.: Новый юрист, 1998. С. 88.
[92] Фролов А.В. Указ. соч. С. 34.
[93] Максимов В.Ю. Указ. соч. С. 80-82; Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. М.: Горячая линия-Телеком, 2002. С. 29.
[94] Максимов В.Ю. Указ. соч. С. 136.

ся в способности программы, независимо от действий пользователя, создавать свои копии и внедрять их в файлы, системные области машинных носителей информации. Причем данные копии могут отличаться от оригинала, но при этом они сохраняют большую часть своих вредоносных функций, в том числе и функцию самораспространения. Функцией самораспространения обладают компьютерные вирусы и компьютерные черви.

Само понятие «компьютерный вирус» ввел в обиход в начале 80-х годов профессор Лехайского университета Фред Коуэн. Такое название было дано рассматриваемому классу программ, очевидно, по причине его сходства с биологическими прототипами с точки зрения возможности самостоятельного размножения. Биологический вирус для функционирования нуждается в живом носителе. Вирусы инфицируют здоровые живые клетки и заставляют их воспроизводить вирус. Таким образом вирус распространяется и на другие клетки.

Одним из первых официально зарегистрированных компьютерных вирусов был так называемый «Пакистанский вирус». Затем появились «Рождественская елка», «Вирус Морриса», «I love you» и другие.

Хорошо известен случай, когда в 1989 году студент американского Корнеллского университета Роберт Моррис в экспериментальных целях создал программу, способную размножаться в сетях, минуя средства обеспечения безопасности. Программа вышла из-под контроля ее создателя и в течение нескольких часов вызвала эпидемию, поразив более 6200 компьютеров, объединенных сетью Интернет. Самым заметным эффектом распространения вируса, кроме необычных сообщений операционных систем, была постоянно возраставшая загрузка пораженных компьютеров. Через небольшой промежуток времени их память была уже полностью перегружена, в результате чего международная сеть оказалась заблокированной около пяти суток, а связь между пользователями прерванной. Общие денежные затраты, связанные с ликвидацией последствий действия вируса, оценивались в сумму, равную почти 100 млн. долларов. Суд над Моррисом был первым в мире судебным процессом над создателем компьютерного вируса[95]. Подобные явления не обошли стороной и Россию.

С распространением персональных компьютеров вирусы поистине стали их бедствием, превратившись в привычную актуальную проблему, породившую целую отрасль информатики – компьютерную вирусологию. Количество вирусов огромно, они пишутся каждый день и практически каждый пользователь компьютера так или иначе сталкивался с их нежелательным воздействием.

Существует множество определений понятия «компьютерный вирус». Большинство из них встречается в технической литературе. Так, например, Касперский Е. В. считает, что вирус – это программа, которая может создавать свои копии, не обязательно совпадающие с оригиналом, и внедрять их в файлы, системные области компьютера, вычислительные сети и т.д.[96] Недостатком

---

[95] Вехов В.Б. Компьютерные преступления. Способы совершения и раскрытия. М.: Право и закон, 1996. С. 85.
[96] Касперский Е.В. Компьютерные вирусы: что это такое и как с ними бороться. М.: СК Пресс, 1998. С. 17.

данного определения является, на наш взгляд, отсутствие указания на наличие вредоносных функций у компьютерного вируса.

А.В. и Г.В. Фроловы называют компьютерным вирусом программу, специально предназначенную для того, чтобы нарушать нормальную работу компьютерных систем[97]. Необходимо отметить, что в своем определении авторы не указали основного свойства компьютерного вируса – способности к самораспространению.

В.И. Ярочкин понимает под вирусом программу, которая обладает способностью размножаться и самовосстанавливаться[98]. Автор выделяет только один из признаков компьютерных вирусов.

В юридической литературе В.Б. Вехов определяет компьютерный вирус как специальную программу для ЭВМ, способную самопроизвольно присоединяться к другим программам («заражать» их) и при запуске последних выполнять различные нежелательные действия: порчу файлов и каталогов (при файловой организации программной среды), искажение и стирание (уничтожение) данных и информации, переполнение машинной памяти и создание помех в работе ЭВМ[99]. Л.Н. Соловьев пишет, что компьютерный вирус – это вредоносная программа для ЭВМ, способная к самораспространению путем включения своего программного кода или некоторой его части в программный код файлов, системные области или иное рабочее пространство машинных носителей информации, с сохранением всех первоначальных свойств или некоторой их части[100].

На наш взгляд, компьютерный вирус – это вредоносная компьютерная программа, способная создавать собственные копии, не обязательно совпадающие с оригиналом, но обладающие свойствами оригинала и способная внедрять эти копии в объекты компьютерной среды. Данное определение, на наш взгляд, содержит все основные характеристики вирусных программ.

Существует значительное число классификаций компьютерных вирусов[101]: по типам объектов, в которые они внедряются (по среде обитания), по особенностям функционирования вируса, по способу заражения среды обитания, по деструктивным возможностям и др.

Кроме компьютерных вирусов к саморапространяющимся вредоносным программам относятся компьютерные черви. В литературе, как в технической, так и в правовой, вопрос выделения компьютерных червей в отдельную группу вредоносных программ является дискуссионным. Ряд авторов, например, В.В. Мельников, В.В. Крылов, Ю.М. Батурин, В.Ю. Максимов, относят такой вид программ к компьютерным вирусам. Другие, В.И. Ярочкин, А.В. Фролов, Г.В. Фролов, Л.А. Соловьев, Е.В. Касперский, выделяют компьютерного червя в самостоятельный класс.

---

[97] Фролов А.В. Указ. соч. С. 39.
[98] Ярочкин В.И. Указ. соч. С. 125.
[99] Вехов В.Б. Указ. соч. С. 78.
[100] Соловьев Л.Н. Указ. соч. С. 29.
[101] См. подробнее: Соловьев Л.Н. Указ. соч.; Максимов В.Ю. Указ. соч.; Козлов В.Е. Указ. соч. и др.

Несмотря на наличие некоторых общих черт, также имеется ряд различий между этими видами вредоносных программ. В отличие от вирусов, черви – это самостоятельные программы. Для размножения они не требуют других программ, в то время как для размножения вирусов требуется носитель (файл или диск). Червь копирует себя в память одного или нескольких компьютеров, связанных между собой в сеть. Данные программы, в большинстве случаев, вообще не обращаются к ресурсам компьютера, за исключением оперативной памяти[102]. Важное различие между червями и вирусами состоит в том, что червь работает в сети, а вирус должен быть физически скопирован, чтобы заразить машину.

Таким образом, компьютерный червь – это вредоносная компьютерная программа способная создавать собственные копии, не обязательно совпадающие с оригиналом, но обладающие свойствами оригинала и способная внедрять эти копии в память одного или нескольких компьютеров, связанных между собой сетью.

Некоторые вирусы и черви относительно безобидны, другие чрезвычайно разрушительны. Многие типичные для персональных компьютеров вирусы, например «Микеланджело», вызывают аварийную остановку компьютера или потерю данных в результате ошибок и других неожиданных взаимодействий с кодом программы. Червь «Рождественская елка» тоже в начале был безобидным. Однако он принял разрушительный характер по мере распространения среди компьютеров, когда стало невозможно выполнять никакую другую работу, и для очищения от инфекции всю сеть пришлось отключать.

В 1988 году червь «Internet Worm» не разрушал данные, но для очистки требовал отключения систем и сетей, что приводило к огромным потерям времени и снижению производительности работы пользователей[103].

В августе 2003 года рекорд по скорости распространения установил Интернет-червь Sobig.F, поразивший сотни тысяч компьютеров во всем мире. Только в США ущерб от его действий превысил 50 млн. долл. Червь парализовал работу сетей в Вашингтоне, прервал деловые процессы в сетях многих крупнейших корпораций[104].

Основной отличительный признак второй группы вредоносных программ – это отсутствие механизма самораспространения. В остальном они наделены аналогичными функциями, что и самораспространяющиеся программы. К этой группе вредоносных программ относятся программные закладки.

Необходимо отметить, что некоторые ученые не относят программные закладки к вредоносным компьютерным программам. Например, В.Ю. Максимов считает, что предметом ст. 273 УК РФ должны быть только вирусные компьютерные программы, остальные программы должны относиться к ведению ст. 272 УК РФ. Основанием для этого, по его мнению, являются особые свойства, характерные для компьютерного вируса, и последствия, вызываемые его

---

[102] См.: Касперский Е.В. Компьютерные вирусы в MS DOS. М.: ЭДЭЛЬ, 1992. С. 8.
[103] Айков Д. Указ. соч. С. 72.
[104] Осипенко А.Л. Указ. соч. С. 86.

действиями[105]. Данное утверждение является спорным и из-за многообразия функций программных закладок, которое не ограничивается организацией неправомерного доступа[106].

Все программные закладки можно условно разделить на несколько групп[107]:

1. Программные закладки, отключающие защитные функции системы – программы, способные модифицировать машинный код или конфигурационные данные системы, тем самым полностью или частично отключая ее защитные функции.

2. Перехватчики паролей – программы, предназначенные для автоматического перехвата имен и паролей, вводимых пользователями защищенной системы в процессе идентификации и аутентификации.

3. Программные закладки, повышающие полномочия пользователя – программы, применяемые для преодоления тех систем защиты, в которых реализовано разграничение доступа пользователей к объектам системы.

4. Логические бомбы – программы, оказывающие при определенных условиях разрушающие воздействия на атакованную систему и обычно нацеленные на полное выведение системы из строя. Программные закладки данного типа вводятся в программное обеспечение и начинают функционировать только при выполнении определенных условий. В качестве таких условий могут выступать: определенные дата и время; запуск непосредственно самой вредоносной программы; число производимых циклов включения и выключения монитора; число запусков программ; запуск и прекращение работы определенных программ; продолжительность работы компьютера и другие. Логические бомбы никогда не используются для организации несанкционированного доступа к компьютерной системе, их основной функцией является полное или частичное разрушение программных средств и данных в компьютерной системе.

5. Мониторы – программы, предназначенные для наблюдения за процессами обработки данных, протекающими в программной среде.

6. Сборщики информации об атакуемой среде – программы, предназначенные для пассивного наблюдения за программной средой, в которую внедрена закладка.

Можно также выделить еще одну группу программных закладок – комбинированные программные закладки[108], так как все рассмотренные выше виды программных закладок могут использоваться как в чистом виде, так и в различных комбинациях. Например, программа, обеспечивающая неправомерный доступ к информации или осуществляющая ее сбор, выполнив свою основную функцию, может быть способна уничтожить данные, с которыми она взаимодействовала, тем самым скрыв следы оказанного воздействия.

Таким образом, за последнее время вредоносные программы получили чрезвычайно широкое распространение и проявили значительное качественное

---

[105] Максимов В.Ю. Указ. соч. С. 8.
[106] Соловьев Л.Н. Указ. соч. С. 31.
[107] См. Белкин П.Ю. Указ. соч. С. 145-147.
[108] Соловьев Л.А. Указ. соч. С. 34.

разнообразие. Данное обстоятельство позволяет классифицировать все вредоносные программы по различным основаниям, что может иметь значение для индивидуализации наказания за незаконный оборот вредоносных компьютерных программ.

2.2. Уголовно-правовые особенности состава преступления, предусмотренного статьей 273 УК РФ

Рассмотрев основные характеристики предмета преступления, связанного с незаконным оборотом вредоносных программ, считаем необходимым перейти к анализу состава преступления, закрепленного в ст. 273 УК РФ, для выявления сильных и слабых сторон его законодательной формулировки.

К слабой стороне следует отнести, например, использование в и диспозиции данной статьи при описании предмета преступления множественного числа, подразумевающее, что для привлечения к уголовной ответственности необходимо создать, использовать, распространить не одну, а несколько вредоносных программ. Подобное смешение единственного и множественного числа может привести к фактической декриминализации деяний, а также может служить причиной ошибок, допускаемых в процессе правоприменения.

Как мы уже отмечали в п. 1.1, законодатель определил родовой объект преступлений в сфере компьютерной информации как отношения общественной безопасности и общественного порядка. Видовым объектом преступлений в сфере компьютерной информации является совокупность общественных отношений, обеспечивающих безопасное создание, преобразование, потребление и защиту компьютерной информации, необходимых для нормальной жизнедеятельности общества.

Непосредственный объект преступления, связанного с незаконным оборотом вредоносных компьютерных программ – совокупность общественных отношений, связанных с безопасным оборотом любой компьютерной информации, хранимой и обрабатываемой в компьютере, компьютерной системе или сети.

Предметом преступления, предусмотренного ст. 273 УК РФ является вредоносная компьютерная программа, которую следует рассматривать как разновидность компьютерной информации.

В отличие от других составов преступлений, закрепленных в главе 28 УК РФ, конструкция состава первой части ст. 273 является формальной, так как преступление признается оконченным с момента совершения любого из указанных действий, независимо от наступления общественно опасных последствий. Главным условием является то, что наступление вредных последствий при использовании потенциальными пользователями соответствующих программ должно быть реально возможным[109]. Формальная конструкция состава связана с тем, что само деяние уже настолько общественно опасно для охраняемого объекта, что нет необходимости ожидать наступления последствий для квалификации такого деяния; кроме того, общественно опасные последствия могут быть слишком отдалены во времени от своей причины – общественно опасного деяния; и наконец, данные последствия слишком разнообразны для того, чтобы можно было их предусмотреть и сформулировать в законе.

---

[109] См.: Уголовное право России. Особенная часть: Учебник / Под. ред. А.И. Рарога. М.: Ин-т межд. права и экон., 1996. С. 324.

Действительно, деятельность, связанную с созданием, использованием и распространением любых компьютерных программ, а тем более вредоносных, на наш взгляд, можно рассматривать как источник повышенной опасности.

Если мы обратимся к определению источника повышенной опасности, сформулированному в юридической литературе, то обнаружим указание на такое его свойство, как неподконтрольность[110].

Повышенная опасность деятельности, связанной с оборотом вредоносных компьютерных программ, обусловлена:

Во-первых, высокой вредоносностью такой деятельности, заключающейся в возможности наступления особо тяжких последствий для потерпевшего. Широкая информатизация различных отраслей человеческой деятельности (воздушный транспорт, космос, медицина, банковские системы и др.), с одной стороны, и наличие благоприятной почвы для развития компьютерной преступности, с другой, способствуют, на наш взгляд, повышению уровня вредоносности этой деятельности. В свое время некоторые цивилисты вели дискуссию о повышенной опасности деятельности, связанной с вирусами биологического происхождения. Так, М.М. Агарков предлагал считать повышенно опасной деятельностью производство, хранение и применение «микробиологических препаратов, представляющих опасность заражения»[111], а О.А. Красавчиков указывал на «микробиологические источники повышенной опасности», понимая под этим различные болезнетворные микробы[112]. Сегодня человеку угрожают не только вирусы биологического происхождения, но и компьютерные вирусы и иные вредоносные программы, о разрушительных свойствах которых нами было сказано выше.

Во-вторых, ее неподконтрольностью, заключающейся в невозможности немедленной остановки воздействия источника повышенной опасности в силу его объективных характеристик и повышенной сложности в эксплуатации, требующей специальной подготовки и знаний. При современном уровне развития компьютерной техники время работы большинства компьютерных программ исчисляется долями секунды. Поэтому зачастую вред, причиненный вредоносными программами, становится очевидным уже после завершения работы программы. Остановка воздействия компьютерной программы в момент причинения вреда затруднена или невозможна по двум причинам: ввиду высокой скорости работы современного программного обеспечения; в силу значительного объема и сложности современных программ, для исправления которых требуются высокая квалификация, которой не обладает обычный пользователь, а также значительные временные затраты.

Современная жизнь в большинстве ее аспектов оказалась зависимой от программного обеспечения: от банковских кодов до красных сигналов светофоров, от телефонных сетей, до DVD-плееров, от воздушных подушек автомоби-

---

[110] См.: Собчак А.А. О понятии источника повышенной опасности в гражданском праве // Правоведение. 1964. № 2. С. 145; Ярошенко К.Б. Специальные случаи ответственности за причинение вреда // Библиотечка народного судьи. М., 1977. С. 6 и др.

[111] Агарков М.М. Обязательства из причинения вреда // Проблемы социалистического права. 1936. № 1. С.58.

[112] См.: Красавчиков О.А. Возмещение вреда, причиненного источником повышенной опасности. М., 1966. С. 65-66.

лей до систем управления воздушным транспортом. Практически весь окружающий нас мир управляется программным кодом. Безусловно, развитие коммуникационных систем, программирование служат развитию возможностей человека, но вместе с тем и таит в себе новые опасности.

Объективная сторона этого преступления выражается в создании компьютерных программ, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации, либо копированию информации, хранящейся в компьютерной системе, сети или на машинных носителях.

Под созданием вредоносной компьютерной программы понимается результат деятельности, выразившийся в представлении в объективной форме совокупности данных и команд, предназначенных для функционирования компьютера и других компьютерных устройств с целью уничтожения, блокирования, модификации, копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях.

Деятельность по созданию вредоносной программы включает в себя следующие этапы, которые по сути аналогичны этапам создания любых других программ:

- постановка задачи, определение среды существования и цели программы;
- выбор средств и языков реализации программы;
- написание непосредственно текста программы;
- тестирование и отладка программы;
- подготовка программы к использованию и распространению.

Некоторые авторы в качестве последнего этапа создания вредоносных программ указывают запуск и непосредственную работу (действие) программы[113]. Однако, на наш взгляд, эти действия могут уже рассматриваться как использование или распространение программы и поэтому не относятся к процессу ее создания.

Создание программы является продолжаемым процессом, но уголовная ответственность может наступать лишь с определенного этапа создания вредоносной программы. По нашему мнению, созданной вредоносная программа будет считаться с того момента, когда последовательность команд станет пригодной для непосредственного выполнения без какого-либо предварительного преобразования.

Существует точка зрения, согласно которой созданием программы может считаться также запись ее текста на бумаге[114]. Однако сам по себе текст не несет никакой, даже потенциальной опасности, пока не будет кем-либо переведен в машинный код (в противном случае, вредными можно признать ряд учебников по программированию), кроме того, написание программ с заданными свойствами без их тестирования и отладки под силу лишь узкому кругу специа-

---

[113] См.: Крылов В.В. Указ. соч. С. 43-44; Добровольский Д.В. Актуальные проблемы борьбы с компьютерной преступностью (Уголовно-правовые и криминологические проблемы): Дис. … канд. юрид. наук. Москва, 2005. С. 27.

[114] См.: Добровольский Д.В. Указ. соч. С. 27; Волеводз А.Г. Указ. соч. С. 74-75.

листов. Поэтому, по нашему мнению, такие действия необходимо расценивать как покушение на преступление.

По поводу того, что следует понимать под использованием вредоносной программы, в уголовно-правовой литературе существуют различные мнения. Так, например, А.Н. Попов, А.Г. Волеводз считают, что использование программы – это выпуск в свет, воспроизведение, и иные действия по их введению в оборот.

С.И. Никулин, А.В. Пушкин указывают, что под использованием вредоносных программ следует понимать их введение (установку) в электронную память компьютера.

Первое из приведенных мнений не совсем точное, так как оно ни чем не отличается от распространения вредоносных программ, которое в ст. 273 УК РФ выделено отдельно и поэтому под использованием таких программ понимается нечто другое.

Во втором случае введение вредоносной программы в чужой компьютер также равносильно ее распространению.

На наш взгляд, под использованием вредоносной программы следует понимать применение этих программ по прямому назначению, для осуществления ею тех функций, для которых она предназначена.

Распространение программы – это предоставление доступа к воспроизведенной в любой материальной форме компьютерной программе, в том числе сетевыми и иными способами, а также путем продажи, проката, сдачи внаем, предоставления взаймы, а равно создание условий для самораспространения программы. Распространение вредоносных программ может осуществляться непосредственно путем их копирования на компьютер потерпевшего, например с диска, а также опосредовано, путем передачи по электронной почте, по линии связи законного пользователя через компьютерную сеть.

Однако, следует иметь ввиду, что не любой оборот вредоносных компьютерных программ является уголовно наказуемым. Исследуемая статья Уголовного кодекса не должна толковаться как влекущая за собой наступление уголовной ответственности в тех случаях, когда совершение деяний, перечисленных в этой статье, связано, например, с разрешенным испытанием, защитой компьютерных систем, интересами науки и другими общественно полезными целями. Также, не подлежат уголовной ответственности при использовании таких программ разработчики антивирусного оборудования, при наличии соответствующей лицензии на данный вид деятельности. Поэтому нам представляется целесообразным сформулировать название ст. 273 УК РФ следующим образом «Незаконный оборот вредоносных компьютерных программ», а диспозицию ч. 1 этой статьи, дополнить словом «незаконные», как это сделано в случаях оборота других общеопасных предметов, оговорив в соответствующих нормативных актах случаи законного обращения с вредоносными компьютерными программами.

Для повышения эффективности борьбы с негативными явлениями, связанными с преступностью в сфере компьютерной информации, специалисты предлагают запретить определенные потенциально опасные действия

еще на этапе, предшествующем совершению преступлений. Большинство преступлений в сфере компьютерной информации требуют предварительной подготовки и владения специальными средствами доступа или иными устройствами. К таким средствам, в частности, относятся компьютерные программы, которые могут свободно распространяться в глобальных сетях. В определенном смысле можно говорить о появлении своего рода «черного рынка» вредоносных программ и устройств взлома.

Разработчики Конвенции по борьбе с киберпреступностью, например, посчитали необходимым выделить в качестве самостоятельного состава преступления умышленное совершение следующих действий (ст. 6): производство, продажа, приобретение для использования, владение с намерением использования, импорт, оптовая продажа или иные способы предоставления в пользование устройств, включая компьютерные программы, разработанные или адаптированные для целей совершения компьютерного преступления; а также компьютерных паролей, кодов доступа и иных подобных данных, с помощью которых может быть получен доступ к компьютерной системе в целом или к ее части, с намерением использовать их для совершения компьютерного преступления. В п. 2 данной статьи отмечается, что лицо не подлежит уголовной ответственности в тех случаях, когда перечисленные выше действия не имеют целью совершение преступления, а связаны, например, с разрешенным испытанием или защитой компьютерных систем[115].

В отечественной уголовно-правовой литературе также высказываются мнения о дополнении перечня деяний, составляющих объективную сторону ст. 273 УК РФ. Например, В.Ю. Максимов считает явным пробелом законодательной техники отсутствие в этом перечне таких деяний, как приобретение и хранение компьютерных вирусов. В подтверждение своих доводов Максимов отмечает, что для всех общеопасных предметов раздела IX в соответствующих статьях присутствует упоминание об их хранении и приобретении[116].

Отдельную проблему представляет собой открытое размещение в глобальных сетях подробнейших описаний тактики и методики применения хакерского инструментария для достижения противоправных целей. По некоторым оценкам, более 400 тыс. Интернет-страниц содержат изложения различных способов реализации компьютерных взломов и сокрытия следов с детально разобранными примерами[117].

Существует и проблема открытого обсуждения так называемых «дыр» систем сетевой безопасности. Многие эксперты полагают, что распространение такой информации в Интернете помогает системным администраторам лучше понять степень угроз и способы их устранения. Однако нередко подобными материалами пользуются и хакеры для создания новых вредоносных программ.

---

[115] Hammond A. The 2001 Council of Europe Convention on cyber-crime: an efficient tool to fight crime in cyberspace? Santa Clara University. Cedric J. Magnin. June, 2001. P 59.
[116] См.: Максимов В.Ю. Указ. соч. С. 96-97.
[117] Осипенко Л.А. Указ. соч. С. 121.

Наконец, угрозу представляет и публикация информации о способах взлома сетей, которую в отдельных, случаях можно квалифицировать как подстрекательство к совершению преступлений в сфере компьютерной информации. В США имеется практика привлечения к уголовной ответственности за «распространение рекомендаций по взлому компьютерных сетей»[118].

А один из законопроектов, разработанный в США, предлагал считать пособниками компьютерных преступников не только тех, кто связан с ними напрямую или укрывает их, но даже тех, чьи советы использовались при совершении преступлений.

На практике применение подобных норм представляется весьма проблематичным. Довольно часто компьютерные средства, созданные для достижения противоправных целей, могут выполнять и определенные полезные функции. При этом усложняется доказывание того, что они разрабатывались исключительно для совершения преступления. И напротив, некоторые легально распространяемые программные средства в определенных обстоятельствах могут быть использованы для нанесения вреда компьютерным системам.

В то же время не вызывает сомнений необходимость установления уголовной ответственности за приобретение и хранение вредоносных компьютерных программ в целях их дальнейшего использования и распространения (как это сделано, например, в ст. ст. 138, 228, 234, 242 УК РФ). В данном случае нельзя согласиться с мнением В.Ю. Максимова о том, что в силу особой опасности подобных программ для компьютерного мира признак цели теряет свое значение и не может быть учтен[119].

Под приобретением необходимо понимать добычу, получение, переход любым способом вредоносной программы от одного лица в полную собственность, владение, распоряжение другого. Например, копирование в память компьютера через сеть, передача программы вместе с машинным носителем в результате акта дарения, мены, купли-продажи, дачи взаймы и т.д. Приобретение окончено с момента перехода вредоносной программы в реальное обладание получившего ее лица.

Под хранением вредоносной программы следует понимать процесс владения, содержание в сохранности, фактическое обладание указанной программой, как своей собственной, так и принадлежащей другим лицам. Особенностью хранения является то, что данное деяние является бездействием, а также то, что это длящийся процесс, который будет завершен в момент, когда предмет преступления окончательно выйдет из владения виновного лица. Для наступления уголовной ответственности лицо должно сознавать факт вредоносности хранимой или приобретаемой программы.

Тяжкие последствия, наступление которых является квалифицирующим признаком ч. 3 ст. 273 УК РФ, относятся к оценочной категории. Отнесение преступных последствий к тяжким входит в компетенцию суда. Согласно п. 8 Постановления Пленума Верховного Суда РФ от 29 апреля 1996 года №1 «О су-

---

[118] См.: «Web Bandit» Hacker Sentenced to 15 Months Imprisonment // Press Release of U. S. Department of Justice. 1999/ Nov., 19.

[119] См.: Максимов В.Ю. Указ. соч. С. 102-103.

дебном приговоре», признавая подсудимого виновным в совершении преступления по признакам, относящимся к оценочным категориям (тяжкие или особо тяжкие последствия, крупный или значительный ущерб, существенный вред, ответственное должностное положение подсудимого и др.), суд не должен ограничиваться ссылкой на соответствующий признак, а обязан привести в описательно-мотивировочной части приговора обстоятельства, послужившие основанием для вывода о наличии в содеянном указанного признака[120].

А.Н. Попов считает, что тяжесть последствий устанавливается применительно к конкретной ситуации. Тяжкими признаются любые последствия, которые суд, с учетом конкретных обстоятельств дела, может признать таковыми. Последствия же могут выражаться в различных формах – вынужденном прекращении деятельности юридического или физического лица, потерей информации и т.д.[121]

По мнению С.В. Бородина к тяжким последствиям, наступившим по неосторожности, могут быть отнесены, например, гибель людей, причинение вреда их здоровью, дезорганизация производства на предприятии или в отрасли промышленности, дезорганизация деятельности банка либо системы банков, осложнение дипломатических отношений с другим государством, возникновение вооруженного конфликта[122].

С.А. Пашин полагает, что под тяжкими последствиями создания, использования и распространения вредоносных компьютерных программ понимаются безвозвратная утрата особо ценной информации, выход из строя важных технических средств (например, систем оборонного назначения, аэронавигационной техники), повлекший за собой несчастный случай с людьми, аварии, катастрофы[123].

Как мы уже отмечали, деятельность, связанную с оборотом вредоносных компьютерных программ необходимо считать источником повышенной опасности. Особенностью вредоносных программ является то, что процесс причинения вреда чаще всего происходит без участия человека, лишая его возможности контролировать этот процесс. Это обстоятельство нередко приводит к причинению большего вреда, чем тот, который ожидался виновным. Поэтому перечень тяжких последствий может быть расширен, в зависимости от конкретной ситуации.

В УК РФ до 2011 года отдельно был криминализирован только один признак, который характерен для многих преступлений против общественного порядка и общественной безопасности – тяжкие последствия. Однако, существовали и некоторые другие признаки преступления, связанного с незаконным оборотом вредоносных программ, существенно повышающие степень общественной опасности данного деяния и поэтому требующие их отдельной криминализации. Федеральным законом № 420-ФЗ от 07.12.2011, статья 273 была до-

---

[120] Бюллетень Верховного Суда РФ. 1996. №1; 2007. №5.

[121] См.: Комментарий к Уголовному Кодексу РФ / Под ред. В.И. Радченко. М.: Вердикт, 1996. С. 490.

[122] См.: Комментарий к Уголовному Кодексу РФ / Под ред. А.В. Наумова. М.: Юрист, 1996. С. 666.

[123] См.: Комментарий к Уголовному кодексу Российской Федерации / Под. общ. ред. Ю.И. Скуратова и В.М. Лебедева. М.: Инфа-М-Норма, 1999. С. 705.

полнена пунктом, в котором квалифицировались деяния, предусмотренные частью первой данной статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности.

Любые групповые преступления всегда признавались наиболее опасными формами преступной деятельности, поэтому во многих статьях Особенной части УК, особенно по умышленным преступлениям, группа лиц, предварительный сговор, организованная группа признаются квалифицирующим признаком состава преступления.

Под предварительным сговором понимается сговор до начала выполнения действий, составляющих объективную сторону преступления. Для данной разновидности соучастия сговор характеризуется чаще всего уяснением объекта и предмета преступления, иногда способом посягательства, что не может свидетельствовать о прочных связях соучастников. В качестве примера можно привести уголовное дело, возбужденное по признакам преступления, предусмотренного ст. 273 ч. 1 и ст. 146 ч. 2 УК РФ. Суть этого дела состоит в том, что у граждан С. и П., которые являлись учредителями ООО «Н.», возник преступный умысел на извлечение доходов путем реализации копий компьютерных программ, без оформления договора на право их обладания, с целью извлечения выгоды. Указанные лица, вступив в предварительный сговор, занимались распространением лазерных дисков для персональных компьютеров, содержащих программные файлы, специально предназначенные для внесения несанкционированной модификации программного продукта АОЗТ «1С», эмулирующие ключ «HASP», являющегося интеллектуальным средством защиты программы от копирования[124].

Организованная группа является одной из наиболее опасных форм соучастия в преступлении. Под организованной группой понимается два или большее число лиц, предварительно объединившихся для совершения одного или нескольких преступлений. Этой разновидности соучастия свойственны профессионализм и устойчивость. Под устойчивостью организованной группы понимается наличие постоянных связей между членами и специфических методов деятельности по подготовке или совершению одного или нескольких преступлений. Устойчивость организованной группы предполагает предварительную договоренность и сорганизованность.

Под лицами, совершающими данное преступление с использованием своего служебного положения необходимо понимать тех лиц, которые в силу своих должностных обязанностей допущены к управлению компьютерной техникой (операторы ЭВМ, системные программисты, инженеры-электронщики и др.).

В соответствии с примечанием 2 к ст. 272 УК РФ под крупным ущербом в статьях 272-274 УК РФ следует понимать ущерб, сумма которого превышает один миллион рублей.

---

[124] Архив УВД Заводского района г. Орла. Уголовное дело № 64742, 2001.

Субъективной стороной преступления, закрепленного в ст. 273 УК РФ, является психическое отношение преступника к совершаемым действиям (бездействиям) и к наступившим последствиям, предусмотренным в диспозиции данной статьи. К признакам, образующим субъективную сторону преступления, относится вина, мотив, цель преступления и эмоциональное состояние лица в момент совершения преступления.

При анализе субъективной стороны преступления, закрепленного в ч. 1 ст. 273 УК РФ, необходимо отметить существование в уголовно-правовой литературе различных подходов к определению вины, как основного признака субъективной стороны преступления. Среди отечественных ученых практически общепринятым является мнение, что при совершении данного преступления вина лица всегда должна быть выражена в виде прямого умысла[125]. Виновный осознает общественную опасность своих действий и желает их совершения. Действующий Уголовный кодекс определяет, что при формальной конструкции состава преступления, вина должна всегда быть выражена в виде прямого умысла.

Также существует мнение, что преступление, закрепленное в статье 273 УК РФ, может быть совершено и с косвенным умыслом[126]. Однако, с таким мнением нельзя согласиться. Интеллектуальный элемент умысла составляет осознание лицом реальной возможности предмета преступления производить перечисленные в диспозиции статьи действия, что специально оговорено в законодательной конструкции ст. 273 УК РФ словом «заведомо». Волевой элемент вины в данном случае характеризуется обязательным желанием совершить указанные действия или бездействие.

Обязательным признаком субъективной стороны приобретения и хранения вредоносной программы является специальная цель – распространение или использование этой программы. Для других деяний, предусмотренных диспозицией ч. 1 ст. 273 УК РФ, цель не будет иметь значения.

Мотивы совершения преступлений, связанных с незаконным оборотом вредоносных компьютерных программ, могут быть различными – от хулиганских (например, в 2000 г. был взломан сайт Агентства военных новостей, на главной странице которого было выставлено нецензурное послание с оскорблениями в адрес Российской Армии и руководства страны[127]) до политических.

В последнее время взлом наиболее популярных сайтов по идеологическим мотивам получил настолько широкое распространение, что для его обозначения в западных средствах массовой информации применяется отдельное понятие — «хактивизм». При этом, как правило, на главной странице серверов размещаются политические воззвания и лозунги, либо блокируется

---

[125] См., например: Максимов В.Ю. Указ. соч. С. 101; Волеводз А.Г. Указ. соч. С. 76; Уголовное право РФ. Особенная часть: Учебник / Под ред. Б.В. Здравомыслова. М.: Юрист, 1996. С. 363; Уголовное право. Особенная часть / Под ред. А.И. Рарога. М.: «Триада, ЛТД», 1996. С. 220; Комментарий к Уголовному кодексу Российской Федерации. Особенная часть / Под ред. Ю.И. Скуратова и В.М. Лебедева. М., 1996. С. 415.

[126] Уголовное право. Особенная часть / Под. ред. Г.Н. Борзенкова и В.С. Комиссарова. М.: Олимп, 1997. С. 544.

[127] См.: Сайт Агентства военных новостей атаковали компьютерные террористы // Агентство военных новостей. 2000. 29 марта.

работа серверов, принадлежащих политическим партиям или известным корпорациям.

В 1998г. было зарегистрировано шесть значительных случаев хактивизма, среди которых блокирование в Интернете доступа к банковским учреждениям Мексики и взлом сервера Атомного центра Индии в знак протеста против испытаний ядерного оружия.

Известен случай, когда хакерская группа Legion of the Underground объявила «войну» Китаю в знак протеста против вынесения смертного приговора двум китайским хакерам. Были взломаны многочисленные серверы, обслуживающие информационную инфраструктуру этой страны[128].

Хактивизм не следует смешивать с явлением, которое в странах Запада окрестили кибертерроризмом. Эти два направления противоправной деятельности в глобальных компьютерных сетях преследуют разные цели, используют разные методы. «Хактивисты» в основном пытаются привлечь внимание общества к политическим лозунгам или проблемам, которые их волнуют. Совершаемые противоправные действия не ведут к насилию и разрушениям.

Напротив, кибертерроризм характеризуется стремлением к существенной дестабилизации общественного порядка. Это явление неразрывно связано с развитием информационной инфраструктуры: при постоянно возрастающей зависимости общества от бесперебойного функционирования вычислительных систем действия, направленные на их разрушение, наносят все более значительный ущерб и вызывают серьезный общественный резонанс[129]. В 2000-2001 гг. было зафиксировано около 1300 серьезных кибератак против вычислительных систем правительственных учреждений, крупных корпораций, стратегических объектов и ведомств США, в том числе Пентагона и ФБР. Атаки становятся все более организованными и профессиональными. Кибертеррористы совершают взломы вычислительных систем, применяют различные вредоносные программы, блокирующие системы или уничтожающие содержащиеся в них данные. Арсенал используемых средств постоянно пополняется и модернизируется в соответствии с изменяющимися условиями, появлением новой техники и технологий.

Анализ изученных уголовных дел, возбужденных за совершение преступлений, связанных с незаконным оборотом вредоносных компьютерных программ, позволяет утверждать, что большинство подобных преступлений имеют корыстную мотивацию (89%). Толковый словарь В. Даля определяет корысть, как страсть к приобретению, к наживе, добыче. Корысть как мотив преступления, связанного с незаконным оборотом вредоносных программ – это стремление извлечь материальную выгоду для виновного или других лиц, в судьбе которых заинтересован виновный, или намерение избавиться от материальных затрат. Иная личная заинтересованность как мотив незаконного оборота вредоносных компьютерных программ может быть выражена в жела-

---

[128] См.: Осипенко А.Л. Указ. соч. С. 92-94.

[129] См.: Мотуз О.В. Виртуальный терроризм – реальность нашего времени // Защита информации: Конфидент. 1999. № 1-2 (25). С. 69.

нии субъекта извлечь из своих действий выгоду неимущественного характера. Для признания рассматриваемого преступления корыстным или совершенным из иной личной заинтересованности необходимо установить, что корыстный или иной личный мотив на его совершение возник у виновного до осуществления преступного деяния и обусловил его.

Хулиганские побуждения при совершении компьютерных преступлений были выявлены при изучении 6% уголовных дел.

Мотивом мести преступники руководствовались в 3% изученных нами материалов уголовных дел. Преимущественно, совершая неправомерные действия, лица пытались отомстить за необоснованное, по их мнению, увольнение с работы.

Любопытство как мотив преступления было выявлено в 2% дел.

В части 3 ст. 273 УК РФ предусмотрена двойная форма вины, которая возможна только в материальных составах. Двойная форма вины заключается в объединении двух форм вины в одном преступлении, то есть по отношению к преступному деянию это умышленная форма вины (для данного состава – прямой умысел), а по отношению к наступившим последствиям – неосторожность.

Законодатель прямо не указывает на наказуемый вид неосторожности, что приводит многих авторов к необходимости либо соглашаться с тем, что при совершении преступления, ответственность за которое предусмотрена ч. 2 ст. 273 УК РФ, уголовно наказуемыми являются оба вида неосторожности, либо остановить свой выбор на одном из видов неосторожности.

Так, Ю.М. Батурин и А.М. Жодзишский считают, что не имеет большого значения, компьютерная ли неграмотность (в данном случае недальновидность, непредусмотрительность) или легкомысленное обращение с компьютерной системой, вызывающее риск, повлекло за собой общественно опасные последствия. И легкомыслие и небрежность могут положить начало событиям катастрофическим[130].

С.А. Пашин считает, что лицо, создавшее или использовавшее вредоносную программу, либо распространившее ее через третьих лиц, отвечает за возникшие тяжкие последствия, если оно предвидело возможность наступления этих последствий. Преступная небрежность в данном случае не вменяется в вину, т.к. между созданием, использованием и распространением вредоносной программы и наступлением соответствующих тяжких последствий такая сложная причинно-следственная связь, что субъект не может полностью предвидеть наступления столь общественно опасного результата[131].

На наш взгляд на квалификацию незаконного оборота вредоносных компьютерных программ, повлекшего по неосторожности тяжкие последствия, не влияет в результате преступного легкомыслия или преступной небрежности наступили эти последствия. Важным является только неосторожность по отношению к наступившим последствиям.

---

[130] Батурин Ю.М. Компьютерные преступления и компьютерная безопасность / Ю.М. Батурин, А.М. Жодзишский. М.: Юрид. лит., 1991. С. 32.

[131] Комментарий к Уголовному кодексу Российской Федерации / Под. общ. ред. Ю.И. Скуратова и В.М. Лебедева. М.: Инфа-М-Норма, 1999. С. 705.

Если в отношении тяжких последствий присутствует прямой или косвенный умысел, то преступление, предусмотренное ст. 273 УК РФ, будет выступать как способ совершения иного преступления и квалификация должна проводиться по совокупности ч. 1 или 2 ст. 273 УК РФ с иными статьями УК РФ.

В случае, если действие вредоносной программы было условием совершения другого преступления, содеянное подлежит квалификации по совокупности вне зависимости от степени тяжести другого преступления.

Субъект рассматриваемого преступления – общий. Им может быть любое вменяемое физическое лицо, достигшее 16-летнего возраста. Мировая практика показывает, что подобные преступления часто совершаются лицами, не достигшими возраста, с которого может наступать уголовная ответственность. Это связано с негативной составляющей влияния глобальных компьютерных сетей на формирование психологических установок несовершеннолетних. Отсутствие сформировавшейся нравственной позиции у подростков приводит к тому, что при посещении сайтов и конференций определенной направленности у них может выработаться позитивное отношение к преступлениям в сфере компьютерной информации и иным видам противоправной деятельности. Опрос 47 235 американских школьников, проведенный агентством Scholastic Inc., показал, что до 48% подростков не осуждают взлом компьютерных сетей. Предпринятое американскими специалистами исследование показало, что подростки, у которых есть серьезные проблемы с родителями или со сверстниками в школе, сильнее подвержены зависимости от Интернета, чем их более благополучные сверстники.

Огромная вычислительная мощность сегодняшних персональных компьютеров позволяет несовершеннолетним лицам совершать противоправные деяния, последствия которых могут быть очень серьезными. Например, обычные преступления в отношении собственности с участием подростков, как правило, включают мелкие кражи в магазинах, различные формы воровства. Использование Интернета позволило некоторым несовершеннолетним участвовать в очень сложных мошенничествах.

Правоохранительными органами зарубежных стран зарегистрировано значительное число случаев, когда малолетние преступники осуществляли торговлю похищенными номерами кредитных карт, получая преступные доходы, измеряемые тысячами долларов. Подростки разрабатывают и распространяют компьютерные вирусы, заражающие десятки тысяч компьютеров, что приводит к тяжелым последствиям. Например, в Болгарии, которая является активным производителем компьютерных вирусов, из 30 выявленных авторов 24 оказались школьниками[132].

Как нами было отмечено ранее, деятельность, связанную с созданием, использованием и распространением вредоносных компьютерных программ, необходимо рассматривать как источник повышенной опасности. В то же время представляется, что обучение основам компьютерной этики в рамках школьно-

[132] См.: Домозетов Х. Социологические проблемы компьютерного пиратства // Социологические исследования. 1997. № 11. С. 111.

го предмета «Информатика» позволяет подросткам осознавать к каким отрицательным последствиям, может привести их неправомерное поведении в сфере компьютерных технологий. Поэтому, на наш взгляд, было бы целесообразно снизить возраст уголовной ответственности по ст. 273 УК РФ до 14 лет и внести в ст. 20 УК РФ соответствующие изменения.

Что касается санкции ст. 273 УК РФ, то необходимо отметить, что материалы изученной судебной практики показывают тенденцию частого применения судами при вынесении обвинительного приговора положений ст. 64 УК РФ. Размер наказания должен быть, прежде всего, необходимым для достижения целей восстановления социальной справедливости, исправления осужденного и предупреждения совершения новых преступлений. Очевидно поэтому, законодатель в 2011 году существенно расширил санкцию ст. 273 УК РФ, предоставив суду возможность наиболее гибко индивидуализировать наказание, а также в полной мере учитывать характер и степень общественной опасности совершенного деяния и особенности личности преступника.

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПНОСТИ, СВЯЗАННОЙ С НЕЗАКОННЫМ ОБОРОТОМ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ

3.1. Специфика причинного комплекса преступности, связанной с незаконным оборотом вредоносных компьютерных программ

Само по себе выявление фактической картины преступности и ее развития еще не дает ответ на вопрос, что же делать. Между этапом познания, оценки преступности и организации борьбы с ней обязателен этап выявления детерминации и причинности преступности. Причинная связь (причинность) есть объективно существующее отношение между явлениями, при котором одно или несколько взаимодействующих явлений (причина) порождает другое явление (следствие)[133]. Различные виды закономерной зависимости между явлениями охватываются понятием детерминация. Соответственно, понятие детерминации шире понятия причинной связи, вместе с тем последнее является более конкретным и содержательным.

Сложный механизм причинной связи в криминологии складывается в результате взаимодействия причин и условий, главных и второстепенных причин, закономерных и случайных событий.

Н.Ф. Кузнецова указывает, что причины и условия объединяются родовым понятием «криминогенные детерминанты»[134]. Под условиями нужно понимать те явления и факты реальной действительности, которые прямо преступлений не вызывают, но наличие которых может способствовать возникновению у человека намерения совершить преступление. Эти условия могут присутствовать или отсутствовать, равно как и преступление может быть совершено, а может и нет. Так, отсутствие замков на дверях склада материальных ценностей — бесспорное условие, способствующее совершению преступлений, однако кражи с этого склада может и не быть.

Выявлять условия преступности легче, чем ее причины, поскольку во многих случаях они лежат как бы на поверхности. Ликвидация условий, способствующих совершению преступлений, как правило, не требует больших материальных затрат, но имеет немаловажное значение. Вместе с тем многие ее недооценивают, скептически относясь к конкретной профилактической деятельности.

Преступное поведение как разновидность сознательного поведения порождается негативными сдвигами в сознании, его деформациями. Последние же не даны людям от рождения, а формируются социальными деформациями общества (экономическими, правовыми, политическими), межнациональными конфликтами и другими объективными воздействиями. Эти негативные социальные факторы безусловно влияют на преступность, но их воздействие не является непосредственным. По отношению к преступности они определяются

---

[133] Кудрявцев В.Н. Причины преступности в России: Криминологический анализ / В.Н. Кудрявцев, В.Е. Эминов. М.: Норма, 2006. С. 9.

[134] Криминология / Под. ред. Н.Ф. Кузнецовой, Г.М. Миньковского. М., 1994. С. 7.

как условия, формирующие причину, в отличие от иной группы условий, способствующих действию уже сложившихся деформаций в сознании[135].

В данном исследовании характеристика причинного комплекса, детерминирующего преступность в сфере компьютерной информации, в том числе преступность, связанную с незаконным оборотом вредоносных компьютерных программ, основывается на социально-психологической концепции причинности, а, следовательно, основными его характеристиками являются разнообразные деформации (дефекты) общественного сознания (психологии) различных уровней.

Поскольку сознание неоднородно, оно имеет свои специфические черты в различных сферах общественной жизни. Эти сферы весьма разнообразны и многочисленны, однако, характеризуя причинный комплекс, остановимся на наиболее значимых из них. При этом следует иметь в виду, что фактически, при описании криминогенных детерминант преступности, связанной с незаконным оборотом вредоносных компьютерных программ, речь идет о том же круге процессов и явлений, который детерминирует неблагоприятные тенденции развития преступности в целом. Таким образом, причины и условия преступности, связанной с незаконным оборотом вредоносных компьютерных программ, являются негативными элементами системы общественных отношений, функционирующей в современном обществе.

Переходя к анализу комплекса причин преступности, связанной с незаконным оборотом вредоносных программ, необходимо отметить, что его особенность заключается в формировании мотивации субъекта и решения совершить подобное преступление под влиянием изменений, связанных с переходом мирового сообщества на новые технологические средства производства и информационного обеспечения. Взаимосвязь и взаимообусловленность новой социальной среды, соответствующих личностных характеристик субъекта и условий социального контроля образуют специфику причинного комплекса детерминации такой преступности.

Наиболее благоприятным для совершения преступлений, связанных с незаконным оборотом вредоносных компьютерных программ, был переходный период в развитии нашей страны. Это время отличалось крайне выгодными для совершения подобных преступлений условиями: отсутствие законодательства регулирующего отношения в сфере безопасности обращения компьютерной информации; отсутствие в правоохранительных органах специальных подразделений, предназначенных для борьбы с таким видом преступности, отток квалифицированных кадров; недостаточность мер по обеспечению безопасности эксплуатируемых компьютерных систем и сетей среди их пользователей, связанная с нежеланием нести дополнительные материальные затраты.

Преступность, связанная с незаконным оборотом вредоносных компьютерных программ, в любых своих проявлениях представляет собой прежде всего преступный бизнес, в основе которого лежат главным образом экономиче-

---

[135] См.: Кузнецова Н.Ф. Проблемы криминологической детерминации. С. 20-24; Криминология / Под ред. Н.Ф. Кузнецовой, Г.М. Миньковского. М., 1998. С. 157-164.

ские причины, т.е. среди различных деформаций общественного сознания, детерминирующих такую преступность как свое следствие, одно из основных мест занимают дефекты, сформированные в его экономической сфере.

Деформации экономического сознания на уровнях группового и индивидуального сознания наиболее часто проявляются в различных разновидностях корысти (служебная, корысть-накопительство и др.); убеждении в невозможности правомерными путями решить стоящие перед группой или индивидом экономические проблемы, а также в том, что обеспечить достойный уровень жизни можно только неправомерными средствами.

Вместе с тем произошли коренные изменения мировоззренческих установок, идеологических ориентаций, касающихся, в том числе, и экономической сферы. Так, ранее осуждаемая частнособственническая психология превращается в признанную и поощряемую систему взглядов и ценностей. Наблюдается несоответствие экономического сознания, психологии и менталитета подавляющего большинства людей изменившейся экономической реальности.

Рыночные отношения основаны на конкуренции, а значит – на подавлении конкурентов, на запрограммированной избыточности рабочей силы, т.е. безработице, на выжимании прибыли в возможно больших размерах, на столь же запрограммированном имущественном и социальном расслоении населения. Экономические ситуации (инфляция, рост цен, низкая оплата труда) неизбежно оказывают влияние на мотивы поведения людей, сказываются на принятии ими решений, в том числе и преступного характера. Например, к моменту экономической либерализации уровень преступности в стране был уже на 80 % выше, чем в 1988 г. Период относительного улучшения криминальной обстановки с 1994 по 1997 г. сменился очередным ухудшением после кризиса в 1998 г. это тревожное время продлилось вплоть до 2000 г., когда уровень общей преступности незначительно упал. Тенденция на повышение общего уровня преступности сохраняется. Как показывают исследования некоторых ученых, со снижением уровня безработицы происходит замещение насильственных преступлений корыстными[136]. Следовательно, можно ожидать дальнейший рост преступлений, связанных с незаконным оборотом вредоносных компьютерных программ, во время устойчивого экономического роста в России.

Изменения, связанные с новым витком техноэволюции, характеризующиеся повсеместным и всесторонним внедрением новых технологий, привели к техническому оснащению отдельных преступников и организованных преступных формирований. Компьютеризация общества привела к появлению новых технологий совершения преступлений. В настоящее время многие традиционные преступления невозможно совершать или масштабно, или без риска быстрого разоблачения, если не использовать высокие технологии. Поэтому банковские сейфы все чаше опустошаются посредством неправомерного доступа в автоматизированные системы межбанковских расчетов, а магазины – через Интернет с помощью системы электронных платежей. Формирование информаци-

[136] См., например: Андриенко Ю.В. В поисках объяснения роста преступности в России в переходный период: криминометрический подход // Экономический журнал ВШЭ. 2001. № 2. С. 194-220.

онного пространства, основанного на использовании компьютерных систем и их сетей, а также взаимосвязанные с этим процессы зарождения и развития общественных отношений в сфере компьютерной информации стали основой возникновения новых видов преступной деятельности.

В обыденном сознании утрачена ценность продуктивного труда как источника благополучия и главного средства самореализации личности; широко распространились представления о возможности легко достигнуть благополучия преступным путем.

Деформации политической психологии играют немаловажную роль в причинном комплексе преступности, связанной с незаконным оборотом вредоносных компьютерных программ. В частности, это проявляется в распространенном заблуждении, что демократия – это вседозволенность, а демократическое общественное устройство несовместимо с сильной государственной властью. Государство, вследствие существующих противоречий между ветвями власти, проявлений национализма, сепаратизма, местничества и корыстолюбия высших чиновников утратило важные рычаги обеспечения единой законности и конституционного правопорядка. Не случайно в общественном сознании сложились представления о том, что государственную власть в стране осуществляет криминальные структуры. Растет неверие в устойчивость государственных институтов, стабильность власти, ее способность обеспечить нормальную жизнедеятельность общества, правопорядок, защиту прав и интересов граждан.

Политическая нестабильность переходного периода выявила недостатки государственной политики в информационной сфере, обострила до предела экономическую и социальную ситуацию, «взорвала» межнациональные отношения, привела к ослаблению, если не к полной дестабилизации всей правоохранительной системы, и, в итоге, к беспрецедентному росту преступности, появлению ее новых видов. Самая суровая в мире советская система уголовного наказания, содержавшая в заключении около 2 млн. человек (0,7% населения) в середине 1980-х гг., вместе с правоохранительной системой были не в состоянии что-либо противопоставить криминалу после демократической революции в обществе[137].

Другой ведущей сферой в общественном сознании является сфера правосознания, деформации которого выступают сопричиной криминальной мотивации всех совершаемых преступлений, в том числе связанных с незаконным оборотом вредоносных компьютерных программ. Одними из условий, формирующими эту причину являются недостатки уголовного законодательства, регулирующего отношения в сфере безопасности компьютерной информации.

Деформации современного правосознания нередко проявляются в правовом нигилизме, негативном отношении к праву, правовой неграмотности, потере ориентиров правомерного поведения, в неверии в его возможность выступать эффективным регулятором общественных отношений, в безразличном или положительном отношении к противоправным деяниям, в устаревших взглядах на проблему преступлений в сфере компьютерной информации в целом, на

[137] Андриенко Ю.В. Указ. соч. С. 197-198.

вредоносные программы в частности, в непонимании общественной опасности последних, в твердом убеждении отсутствия равенства граждан перед законом, в недоверии к системе правоохранительных и судебных органов.

Нравственное сознание тесно связано с правосознанием, а также со многими сферами жизнедеятельности, поскольку, представляя собой систему знаний и принципов о добре и зле, совести, долге, чести, ответственности в межличностных отношениях, выступает регулятором этих отношений и соответствующего поведения. Среди таких сфер жизнедеятельности можно выделить, в частности, нравственное сознание в сфере экономических, профессиональных, а также в области самосознания и самооценки.

Нравственное сознание пронизывает буквально все сферы жизни человека, как и правосознание, оно определяет рамки дозволенности любого вида поведения людей, но диапазон этих нравственных рамок гораздо шире, чем правовых. Поэтому деформации нравственного сознания, как и деформации правосознания, можно назвать сопричиной совершения большинства, в том числе преступлений, связанных с незаконным оборотом вредоносных компьютерных программ.

Нравственные проблемы современной общественной психологии состоят прежде всего в том, что прежние нравственные ценности и ориентиры в значительной степени отвергнуты (возможно, и не без оснований), а новой прочной системы нравственной регуляции поведения не создано, в результате чего образовались существенные проблемы в этой сфере регулирования.

К сожалению, эти пробелы нередко заполняются не только сомнительными суррогатами, но и откровенно аморальными «ценностями». Сознание многих людей деформировано, противоречиво, поскольку пытается сочетать несовместимые стереотипы и установки. Накопление негативных эмоций, разносторонних раздражителей и стимулов порой достигает запредельного напряжения, часто угрожает криминальным срывом. Все это дополняется неуверенностью в завтрашнем дне, переживании ненадежности социального статуса, материального и служебного положения.

В результате наметилось смещение ценностных ориентаций отдельных слоев общества в сторону идеалов криминальных структур. Основным компонентом набора антиценностей выступает вседозволенность, понимаемая как освобождение от нравственных императивов. Большая вероятность того, что лицо, совершившее преступление, связанное с незаконным оборотом вредоносных компьютерных программ, сможет избежать уголовной ответственности, является одним из основных факторов, порождающих деформации правосознания личности. Если преступность высока, а преступления часто безнаказанны (как это имеет место с преступностью исследуемого вида), возникает особое психологическое состояние допустимости, разрешенности преступных действий, а также представление о слабости, ничтожности законов, в результате чего граждане легко склоняются к противоправному, в том числе и преступному, поведению, ориентируясь на бездействие и слабую эффективность правоохранительной системы. Подтверждением безнаказанности компьютерных преступников является высокий уровень латентности преступлений

в сфере компьютерной информации. Уровень латентности незаконного оборота вредоносных компьютерных программ составляет около 95%.

На наш взгляд, немаловажной для уяснения причин преступности, связанной с незаконным оборотом вредоносных компьютерных программ, является проблема влияния глобальных сетей при их использовании на поведение пользователей, зачастую противоправное. Глобальные сети являются достаточно специфичной средой проявления общественных отношений. Это связано с тем, что, во-первых, в современных глобальных сетях представлены практически все социальные слои и возрастные группы населения. Здесь в той или иной форме нашли воплощение и большинство видов деятельности общества (политическая, финансово-экономическая, коммерческая, образовательная, культурная и т.д.).

Во-вторых, на основе общности интересов или участия в совместной деятельности в сетях создаются многочисленные группы территориально удаленных субъектов, развиваются неизвестные ранее формы общения и взаимодействия людей, идет процесс формирования сетевой субкультуры, использующей особый язык (жаргон, сленг) и специфические нормы взаимодействия[138]. В таких группах складывается своя внутренняя социальная иерархия, появляются формальные и неформальные лидеры.

В-третьих, появилось значительное число пользователей, отдающих существенную часть своего времени различным формам сетевой деятельности и общения. Данная среда оказывает определенное воздействие на сложившиеся в обществе формы социальных взаимодействий и модели экономической деятельности.

Образованную глобальными компьютерными сетями среду в западной литературе принято называть киберпространством. В русскоязычной литературе встречаются также термины «виртуальное пространство», «виртуальный мир». Понятие «киберпространство» обозначает моделируемое с помощью компьютерного оборудования особое информационное пространство, в котором присутствуют специфические информационные объекты (компьютерные программы, данные и т.п.)[139].

В криминологии проблема взаимодействия личности с социальной средой, воздействия среды на противоправное поведение относится к числу центральных. Под социальной средой следует понимают совокупность всех тех общественных условий, деятельностей и отношений, которые окружают личность и оказывают активное (прямое или косвенное, стихийное или сознательное) воздействие на ее сознание и поведение[140].

Сетевая среда представляет собой устойчивую специфическую совокупность личностей, участвующих в сетевых коммуникационных процессах, и возникающих между ними общественных отношений.

---

[138] См.: Белинская Е.П. Человек в информационном мире // Перспективы социальной психологии. М., 2002.

[139] См.: Collin B.C. The Future of CyberTerrorism // Proceedings of 11th Annual International Symposium on Criminal Justice Issues. The University of Illinois. Chicago, 1996.

[140] Попов С. Сознание и социальная среда. М., 1979. С. 31.

Как и социальная среда в целом, сетевая среда влияет на личностные характеристики людей, социально-психологические характеристики представленных в ней групп, порождает соответствующую мотивацию поведения, избрание конкретных средств достижения целей, в том числе противоправных. А процесс становления социальных отношений и форм собственности в новой информационной среде, не подкрепленный в достаточной мере ни соответствующими законодательными, ни нравственными установками, оказывает существенное влияние на структуру преступности, порождает неизвестные ранее формы негативного девиантного поведения[141]. Доступность приобретения необходимых технических средств, постоянное снижение стоимости подключения к Интернету, развитие льготных форм оплаты приводят к изменению социального состава пользователей и, как следствие, появлению в сети новых криминогенных социальных слоев.

Л.А. Осипенко выделяет те стороны сетевой среды, которые так или иначе связаны с преступным поведением: поддержка социально опасных взглядов; нарушение механизмов детерминации позитивного поведения; влияние на психическое состояние (особенно подростков)[142].

Сегодня сетевое сообщество отличается значительным многообразием индивидов, большой социальной и культурной дифференциацией и стратификацией, широким спектром взглядов на любые общественные проблемы. Между тем изоляция субъекта с нестандартными (в том числе и негативными) установками от нормальных контактов в реальной микросреде в большинстве случаев приводит к тому, что он ищет признания в других местах среди подобных себе[143]. Такой индивид может найти в сетях поддержку и понимание практически в любых взглядах, которые отвергаются его конкретным окружением. Это, безусловно, повышает привлекательность сетевой среды для указанных личностей. Виртуальный мир дает им дополнительную свободу действий и выражения мыслей, эмоций, чувств, ограничиваемую в реальной жизни.

Даже при неглубоком поиске в сети Интернет легко обнаружить сайты, где положительно оцениваются различные негативные явления. Интернет нередко формирует и маргинальные группы людей. Хакерское сообщество выступает лишь как одна из таких групп.

Глобальными компьютерными сетями усиливается процесс опосредованного общения людей, участники которого чаще всего имеют поверхностные, неглубокие межличностные отношения. Это ведет к сокращению влияния ближайшего окружения на личность как средства социального контроля, нарушению механизмов детерминации позитивного поведения. Более того, возможность анонимного участия в сетевом общении формирует у индивидов с неустоявшимися взглядами представление о вседозволенности и ненаказуемости любых проявлений в сетевой среде. Отдельные личности пытаются исполь-

---

[141] См.: Василькова В.В. Порядок и хаос в развитии социальных систем: (Синергетика и теория социальной самоорганизации). СПб., 1999. С. 264.

[142] См.: Осипенко Л.А. Указ. соч. С. 47-56.

[143] См.: Антонян Ю.М. Психология преступника и расследования преступлений / Ю.М. Антонян, М.И. Еникеев, В.Е. Эминов. М., 1996. С. 67.

зовать сетевые возможности, чтобы досаждать людям, с которыми в реальной жизни их связывают неприязненные отношения. Индивиды с различного рода отклонениями в психике могут избирать для себя и случайную жертву, общаясь, например, в чатах.

Сетевая среда способна оказывать влияние и на психическое здоровье личности. Учеными отмечается возникновение у отдельных индивидов болезненного пристрастия к участию в сетевых процессах. Термин «интернет-зависимость» ввел в 1996 г. американский психолог А. Голдберг для описания неоправданно долгого (патологического) пребывания в Интернете. Это является причиной социальной дезадаптации личности. Опрос 18 тыс. пользователей Интернета в США показал, что доля склонных к подобной зависимости личностей достигает 6%, причем патология проявляется в разрушении обычного образа жизни, смене жизненных ориентиров, появлении депрессии, нарастании социальной изоляции[144].

Ранее нами уже упоминалось о возможности негативного влияния глобальных компьютерных сетей на формирование психологических установок несовершеннолетних.

Таким образом, представляется вполне оправданным отнесение глобальных сетей к своего рода криминогенным объектам. К глобальным сетям подключены объекты, в отношении которых возможны преступные посягательства повышенной общественной опасности. При изучении сетевой среды можно обнаружить проявление тройного механизма социальной детерминации преступности: путем определенного социального формирования личности; путем дачи ей предписаний противоправного либо противоречивого характера; путем постановки личности в ситуации, вынуждающие и облегчающие выбор преступного варианта поведения[145].

К условиям, способствующим совершению преступлений, связанных с незаконным оборотом вредоносных программ также можно отнести:

Во-первых, недостатки в деятельности правоохранительных органов (недостаточная квалификация работников правоохранительных органов, слабое техническое и материальное обеспечение подразделений, осуществляющих борьбу с этим видом преступности).

Во-вторых, низкий уровень компьютерной культуры населения. В большинстве случаев потерпевшие сами создают условия для совершения преступлений, которые при должной осмотрительности с них стороны можно было бы предотвратить. Так, одной из основных причин массовых взломов сайтов сети Интернет специалисты считают их откровенно слабую защищенность. Так, представители исследовательской организации Unisus Australia в 2002 году проверили 3 млн. случайно выбранных веб-сайтов, расположенных по всему миру. Оказалось, что 80% из них сравнительно просто взломать или вывести из строя, поскольку на них не используются даже простейшие системы защиты[146].

---

[144] См.: Янг К.С. Диагноз – Интернет-зависимость // Мир Internet. 2000. № 2. С. 24-29.
[145] Осипенко А.Л. Указ. соч. С. 56.
[146] Осипенко А.Л. Указ. соч. С. 92.

Низкий уровень компьютерной культуры у потерпевших имеет следующие проявления:

- отсутствие у потерпевшего единой политики по обеспечению безопасности компьютерной информации от вредоносных программ;
- отсутствие необходимых программных и аппаратно-технических средств защиты компьютерной информации, обеспечивающих защиту от внедрения и воздействия вредоносных программ;
- отсутствие квалифицированных специалистов по противодействию вредоносным программам;
- использование устаревшего или поврежденного программного оборудования, случайных машинных носителей информации;
- неконтролируемый обмен электронными письмами, непроверенными файлами и программными средствами через глобальные сети;
- недостаточная информированность о существующих вредоносных программах и признаках их внедрения и воздействия;
- недостаточная разъяснительная работа в организации или ее отсутствие.

В заключении необходимо отметить, что все вышеназванные причины преступности всегда действуют как система, комплекс сопричин. Различные их сочетания на уровне группового сознания детерминируют, в том числе и преступность, связанную с незаконным оборотом вредоносных компьютерных программ, а на индивидуальном уровне служат базой для формирования криминогенной мотивации, являющейся непосредственной причиной преступного поведения.

Итак, особенностью комплекса причин преступности, связанной с незаконным оборотом вредоносных программ, в частности, заключается в формировании мотивации субъекта и решения совершить подобное преступление под влиянием изменений, связанных с переходом мирового сообщества на новые технологические средства производства и информационного обеспечения.

Ведущую роль в причинном комплексе преступности, связанной с незаконным оборотом вредоносных программ, играют деформации экономического, правового и нравственного сознания, на индивидуальном уровне реализуемые в корыстной мотивации, правовом нигилизме и убежденности в собственной безнаказанности. Формирующими эти причины условиями выступают: переход к информационному обществу, последствия неудачных экономических реформ, недостатки государственной политики в информационной сфере, недостатки уголовного законодательства, регулирующего отношения в сфере безопасности компьютерной информации, разрушение системы нравственных ценностей, низкий уровень компьютерной культуры населения, негативное влияние сетевой среды, недостатки в деятельности правоохранительных органов, высокий уровень латентности компьютерных преступлений.

3.2. Особенности личности преступника, занимающегося незаконным оборотом вредоносных компьютерных программ

Изучение особенностей лиц, совершающих преступления, является важным условием правильной организации борьбы с определенным видом преступной деятельности. Для преступлений, связанных с незаконным оборотом вредоносных программ, изучение личности преступника приобретает особую актуальность, так как в данном случае приходится сталкиваться с субъектами, которые до недавнего времени не попадали в поле зрения правоохранительных органов. Любопытство общества по отношению к этим новым видам преступлений отчасти затеняет связанную с ними опасность, уводит ее на второй план, порождает отношение к компьютерным преступникам как к экзотическому явлению, формирует их искаженные образы, не соответствующие действительности. Поэтому для восстановления реальной картины необходимо уделить внимание психологическим, половозрастным и иным особенностям таких лиц, вероятным мотивам преступления, поведенческим признакам, проявляющимся при подготовке, совершении преступлений и сокрытии следов содеянного.

Анализ уголовных дел, а также специальной литературы позволяет констатировать, что подобные преступления в подавляющем большинстве совершаются лицами мужского пола. Однако, принимая во внимание тенденции в мировой практике можно предположить, что скоро доля женщин в такого рода преступлениях будет увеличиваться[147].

Важнейшим компонентом криминологического портрета компьютерного преступника является возраст, который, несомненно, накладывает свой отпечаток на поведение людей, их потребности и жизненную установку.

Среди преступников данного типа преобладают молодые люди в возрасте от 18 до 24 лет (52% изученных уголовных дел), т.е. возраст студенческой молодежи либо тех, кто закончил вуз, но еще не вступил в брак, возраст первого серьезного карьерного роста. Иными словами, это едва ли не самый важный период социализации человека в обществе, особенно для мужчин, требующий сил, времени и разного рода ресурсов. В научной литературе отмечается, что именно в этом возрасте способность к восприятию информации наиболее высока, что особенно важно для преступлений, связанных с незаконным оборотом вредоносных компьютерных программ. Именно в этом возрасте у таких лиц особенно высока потребность в самоутверждении и стремление получить максимальное количество жизненных благ при отсутствии реальной возможности достичь этого.

Необходимо отметить, что, на наш взгляд, полученные в результате анализа уголовных дел данные не всегда отражают реальное состояние дел, так как в данном случае мы имеем дело только с выявленными правонарушениями. В то же время официальные власти большинства стран, в том числе и США, где

---

[147] По данным социологов США треть арестованных за преступления хакеров были женщины (Кузнецов А. Пираты в Интернете // Милиция. 2000. № 2. С. 27).

подобные преступления расследуются с 1966 года, вынуждены признавать, что выявление правонарушителя в 90% случаях невозможно. По нашему мнению, наиболее опасные преступления подобного вида совершают лица в возрасте от 25 до 35 лет, имеющие техническое образование и продолжительный опыт работы в области информационных технологий, неправомерная деятельность которых практически никогда не бывает наказана. Основная же часть раскрытых преступлений, связанных с незаконным оборотом вредоносных компьютерных программ, совершается специалистами невысокой квалификации, знаний которых не хватает для того, чтобы скрыть следы своего преступления.

Как мы уже отмечали ранее, в последнее время существует тенденция к омоложению компьютерных преступников, что может привести к тому, что в скором времени доля и общественная опасность хакеров, не достигших 16-летнего возраста будет усиливаться по мере роста компьютеризации общества[148]. Среди причин такого омоложения можно отметить потребность в общении в Интернете, в обретении друзей из сетевого сообщества, потребность в знаниях.

Образовательный уровень преступников достаточно высок: около 70 % из них имеют высшее или неоконченное высшее, а также среднее специальное образование.

Важное значение для выявления подобных лиц имеет также определение психологических особенностей их личности. При этом важно не описание всех качеств личности, а выделение ведущих, определяющих характер поведения.

Вопреки образу, формируемому средствами массовой информации, лица, совершающие преступления, связанные с незаконным оборотом вредоносных программ редко принадлежат к «психопатам», помешанным на мировом господстве, а у большинства из них даже отсутствует стремление к лидерству. Пребывание в виртуальном электронном мире становится наиболее значимой частью их жизни, в которой они чувствуют себя более уверенно. Компьютер является для них в определенной степени средством для бегства от действительности.

Как правило, изучаемые лица имеют замкнутый характер, склонны к депрессии, погружены в личные переживания, не стремятся достичь высокого положения в обществе. Во многих семьях хакеров отмечается сложный психологический климат. Нередко у них неполные семьи, сложные отношения со сверстниками. Большинство хакеров склонны к индивидуальным формам деятельности, в общении для них характерны холодность, конфликтность и пониженная эмоциональность.

В противоправных деяниях подобных людей находит проявление затаенная обида на кого-либо или общество в целом, нередки заявления о том, что они стремятся преподать своими действиями урок кому-либо. Довольно часто у них тяжелый характер. Несмотря на это, многие из них имеют ярко выраженную потреб-

[148] Кузнецов А. Указ. соч. С. 27.

ность принадлежать к определенной большой социальной группе, и такая потребность находит реализацию при объединении их в хакерские сообщества.

По мнению специалистов, среди наиболее распространенных качеств таких преступников преобладают правовой нигилизм и завышенная самооценка. Такие лица, ощущая безнаказанность своих противоправных действий, часто пренебрегают требованиями норм права, считают допустимым определять моральность тех или иных правовых норм на основе собственных критериев, часто проявляя определенный инфантилизм, безответственность, непонимание возможных опасных последствий противоправных действий. Как правило, при этом игнорируются интересы социума.

Гипертрофированная самооценка приводит к тому, что отдельные лица совершают противоправные деяния спонтанно, без серьезной предварительной подготовки. Под воздействием «комплекса безнаказанности» они оставляют многочисленные послания руководителям служб безопасности, с гордостью публикуют сообщения о своих противоправных действиях в сетевых конференциях и т.п. Нередко можно встретить и хвастливые описания «побед» с конкретными указаниями на их организаторов в конференциях и чатах. По результатам опросов, проведенных ФБР, до 98% хакеров считают, что их никогда не смогут уличить в хакерстве[149].

Также необходимо отметить, что эти люди, как правило, являются яркими, мыслящими личностями. Для многих из них характерны достаточный уровень квалификации, глубокие познания в области информационных технологий, высокая работоспособность, упорство. Эти сами по себе позитивные качества при выборе субъектом преступных способов достижения целей становятся элементами преступного профессионализма. В частности, высокий интеллект и профессиональная подготовленность позволяют преступнику достаточно полно оценить все возможные препятствия на пути достижения поставленных целей и выбрать оптимальный вариант поведения, просчитав вероятные действия правоохранительных органов.

Предвидение высокой вероятности наступления правовых последствий для многих из таких лиц способствовало бы отказу от совершения преступления. Для таких лиц боязнь ответственности тесно связана со степенью активности правоохранительных органов.

Подготовленность субъекта к реализации преступных замыслов определяется и наличием необходимых навыков. Изучаемые лица наиболее важными считают для себя такие качества, как опыт работы с информационными системами, умение программировать, способность быстро изучать новые языки программирования, умение общаться с людьми, полученное образование. Причем навыки общения, необходимые для сбора предварительных данных о жертве, по их мнению, в отдельных случаях играют решающую роль. Как правило, указанные лица стараются получить максимальный объем знаний о функционировании и механизмах защиты объектов вычислительных систем и быть в курсе самых последних новостей в этой сфере.

---

[149] См.: Осипенко А.Л. Указ. соч. С. 170-173.

Среди их поведенческих признаков могут быть выделены: поддержание связей с хакерскими группами; обсуждение способов совершения преступлений, связанных с незаконным оборотом вредоносных компьютерных программ; регулярное участие в конференциях хакерской направленности; заявления о совершении правонарушений; использование специфического жаргона.

Проблема получения информации о типичных характеристиках личности преступника, совершающего преступления рассматриваемой категории, усугубляется отсутствием достаточного объема эмпирического материала для проведения ее всестороннего анализа.

Необходимо отметить, что в настоящее время совокупность лиц, совершающих преступления по незаконному обороту вредоносных программ, является достаточно разнородной по своему составу. Поэтому стремление построить единый обобщенный портрет всех личностей, совершающих противоправные действия в данной сфере, обречено на неудачу. Тем не менее выделение категории лиц, совершающих подобные преступления, на основе различных критериев, способствует выявлению объединяющих их особенностей.

Например, канадский психолог М. Роджерс, выделил группы преступников в зависимости от уровня их технической подготовленности: новички; киберпанки; свои — служащие организаций-жертв; кодировщики; хакеры старой гвардии; профессиональные преступники; кибертеррористы[150].

Д. Айков делит компьютерных преступников в зависимости от мотивов преступления на три категории: взломщики (основное побуждение – проникновение в систему), преступники (основное побуждение – выгода), вандалы (основное побуждение – нанесение ущерба)[151].

Представляет несомненный интерес и деление, представленное в Указе президента США, направленном на борьбу с компьютерной преступностью. Здесь обозначены три основные группы субъектов: неорганизованные субъекты (сотрудники организаций, хакеры); организованные субъекты (представители организованной преступности, промышленного шпионажа, террористы); представители спецслужб других государств[152].

По мнению многих сотрудников правоохранительных органов западных стран, недовольные служащие и недавно уволенные сотрудники, достаточно подготовленные в области информационных технологий и по роду деятельности имеющие определенные права доступа к вычислительным системам, составляют наиболее значимую в процентном отношении группу киберпреступников. Имеются примеры, когда обиженные увольнением служащие наносили серьезный ущерб функционированию компаний.

Например, в 2002 г. один из бывших сотрудников фирмы UBS Paine-Webber нанес ей ущерб на сумму около 3 млн. долл. Он внедрил в сеть организации через заблаговременно оставленную дыру в программном обеспечении вредоносную программу. Из 1,5 тыс. компьютеров компании было повреждено почти

---

[150] См.: Rogers M. A New Hacker Taxonomy. Winniper, 2000. P. 34-35.
[151] См.: Айков Д. Указ. соч. С. 90-94.
[152] См.: Осипенко А.Л. Указ. соч. С. 149.

две трети. Злоумышленник предполагал получить прибыль за счет падения курса акций компании.

Достаточно большую потенциальную опасность представляют и лица из числа штатных сотрудников: системные программисты, сетевые администраторы, специалисты по защите информации, операторы ЭВМ, инженерный персонал, пользователи системы. Наиболее опасен в этом отношении специалист по защите информации, в силу своих профессиональных навыков способный умело скрыть преступление, а на случай обнаружения имитировать проникновение злоумышленника извне. В целом в правоохранительной практике сотрудников пострадавшей организации принято считать основным субъектом противоправных действий в отношении сетевых объектов.

Однако в последние годы ситуация постепенно меняется. В отчете ФБР и Института компьютерной безопасности США в качестве основного источника опасности для объектов вычислительной техники называются внешние подключения к сети Интернет (в 2001 г. — 74% инцидентов; в 2000 г. — 70%; в 1999 г. — 59%). Аналогичные оценки приводятся и в обзоре, подготовленном Конфедерацией британской промышленности (Confederation of British Industry). Утверждается, что основная угроза исходит не от работников компании, а в большей степени от хакеров, а также от уволенных сотрудников и представителей организованной преступности[153].

Для российского общества проблема участия представителей технической элиты в противоправной деятельности связана и с определенными социальными предпосылками. По мнению специалистов, вероятность совершения сетевых преступлений повышается в тех регионах, где имеется множество подготовленных профессионалов, не получающих соответствующего своим способностям вознаграждения за свою работу.

Серьезную угрозу информационной безопасности могут нести конкуренты или лица, занимающиеся промышленным шпионажем, а также профессиональные преступники и кибертеррористы. Представители этих групп осуществляют противоправную деятельность в широком диапазоне от корпоративного шпионажа до чрезвычайно опасных диверсий против вычислительных систем жизненно важных объектов. Такие лица, как правило, хорошо обучены и имеют доступ к самому современному оборудованию.

Между тем для сотрудников правоохранительных органов особый интерес, как правило, представляют лица, которые могут совершать неочевидные опасные преступления. В этом отношении именно хакеры, как группа, продуцирующая большое число латентных преступлений, выступают достаточно новым и важным в криминологическом плане явлением. Специалисты достаточно высоко оценивают угрозу сетевой безопасности, исходящую от хакеров, которые представляют определенный криминологический феномен, требующий соответствующего осмысления.

Следует отметить, что несмотря на частое использование термина «хакер», среди специалистов до сих пор отсутствует его единое толкование.

---

[153] См.: Осипенко А.Л. Указ. соч. С. 150-151.

Этот термин используется, как минимум, в двух значениях. Первое имеет негативную окраску, определяет личность с противоправными установками, преступника, компьютерного «взломщика»; второе вполне позитивно и подразумевает специалиста в области информационных технологий, профессионала, увлеченного своим делом[154].

Конечно, не стоит ставить знак равенства между хакерами и преступниками, к сообществу хакеров следует относиться как среде, оказывающей существенное влияние на преступность в сфере высоких технологий. В то же время не все виды девиантного поведения в сфере компьютерной информации связаны с хакерами (этот термин более узок, чем «лицо, совершающее преступление в сфере компьютерной информации»). Но, так или иначе, именно хакеры являются ядром преступности, связанной с незаконным оборотом вредоносных компьютерных программ, породившим соответствующую субкультуру[155].

Хакерская среда образует уникальное явление, не имеющее аналогов в правоохранительной практике и лишь по отдельным характеристикам приближающееся к другим криминальным сообществам. Одно из его основных отличий связано с использованием коммуникационных возможностей современных глобальных сетей для обсуждения и координации своей деятельности. С этой целью в глобальных сетях организуются конференции хакерской тематики, создаются хакерские сайты.

Хакерская среда имеет сложную организацию, находится в процессе постоянного развития и еще достаточно слабо изучена. Изучение хакерского сообщества затруднено в связи с явной недостаточностью фактических документированных материалов, отсутствием возможности обычного статистического наблюдения. Это заставляет прибегать к методам косвенного познания, например выявлению и опросу жертв правонарушений, специалистов по защите информации, изучению документов и т. д. Важным источником исходной информации для анализа выступают данные зарубежных исследователей. Представляется эффективным и еще один из методологических приемов: контент-анализ основных каналов общения хакеров — электронных досок объявлений, сайтов криминальной направленности, конференций.

При изучении хакерской субкультуры следует помнить, что она формировалась главным образом в киберпространстве в условиях отсутствия государственных границ и государственного регулирования совершаемых в нем действий. Анализ норм хакерской этики делает очевидным игнорирование основных правовых принципов. Отдельным слоям общества импонирует идеология хакеров, которая сконцентрирована вокруг лозунгов: «информация принадлежит всем», «программы должны быть общедоступными и не должны защищаться авторским правом». Как следствие, снисходительное отношение к хакерам переносится и на совершаемые ими преступления[156].

---

[154] См.: Айков Д. Указ. соч. С. 91.
[155] См.: Осипенко А.Л. Указ. соч. С. 154-155.
[156] Осипенко А.Л. Указ. соч. С. 158.

Вполне естественно, что в таких условиях хакеры ощущают себя особым элитарным сообществом с определенными законами, традициями, солидарностью, поэтому большинство из них причиняют ущерб сетевым объектам в стремлении поддержать такой мнимый престиж.

Хакерское сообщество образовано достаточно разнородной совокупностью индивидов с широким спектром направлений противоправной деятельности, используемых методов и преследуемых целей. Среди хакеров встречаются как любознательные подростки, так и опасные профессиональные преступники. На основании опроса 100 тыс. хакеров дается следующая приблизительная оценка распределения их по уровню квалификации: представители киберкриминала мирового класса — 0,1%; профессиональные хакеры — 9,9%; любители — 90,0%[157].

А.Л. Осипенко предлагает следующую типологию хакеров.

1. Многочисленная группа начинающих хакеров состоит из лиц, слабо разбирающихся в основах программирования и использующих готовые программные средства осуществления атак, зачастую даже не понимая принципов их действия. Для ее обозначения применяется термин «script kiddies». Таких любителей становится все больше, а наносимый ими ущерб превышает тот, который причиняют квалифицированные хакеры.

2. В основной группе хакеров нередко выделяют такие подгруппы, как «крэкеры» (субъекты, специализирующиеся на разрушении средств безопасности сетей или компьютерных систем с целью нелегального использования их ресурсов), «фрикеры» (лица, проникающие в телефонные сети и иные защищенные телекоммуникационные системы). В целом представители типичной группы хакеров имеют неплохие навыки программирования, способны создавать собственное программное обеспечение для взлома, лучше понимают основы функционирования вычислительных систем, на которые осуществляют нападение. Как правило, такие хакеры преднамеренно участвуют в противоправных действиях, связанных с блокированием работы сетевых систем, хищениями номеров кредитных карт, мошенничеством.

3. «Кодировщики» (coders) осуществляют взломы программного обеспечения. Типичный «кодировщик» не продает краденый материал, а распространяет бесплатно через специализированные сайты. Однако не все из них столь бескорыстны, некоторые предлагают платные услуги по взлому программ.

4. Хакеры «старой гвардии» (old guard hackers) в основном имеют высокую профессиональную подготовку при отсутствии прямых преступных намерений. Такие лица с некоторым превосходством относятся к требованиям норм права, считая, что им в сетях дозволено практически все. Они руководствуются в основном исследовательскими интересами.

Достаточно интересным является вопрос о принципах существования хакерских групп. Наибольшее распространение получили хакерские группы, участники которых имеют опосредованные сетевым общением связи и не ведут совместной преступной деятельности. В основном в таких группах об-

[157] См.: IBM Global Security Analysis // Computer World Россия. 1999. № 11. С. 29.

мениваются опытом взлома и устранения его следов, оказывают друг другу моральную поддержку.

Реже встречаются группы с устойчивыми связями. Однако и в них, как правило, совместная деятельность носит случайный характер, отсутствует признанный лидер и распределение ролей, все участники равноправны. Такие группы могут выполнять оплачиваемые заказы на взлом определенных сетевых систем.

Также встречаются и хорошо организованные группы с определенной иерархической системой. По оценкам специалистов, лишь на территории Москвы действует не менее восьми подобных хакерских группировок, в том числе имеющих межнациональные и трансграничные связи.

Особое место в хакерском сообществе занимают warez-группы, специализирующиеся на взломе программного обеспечения. Известны более 10 крупных международных группировок, осуществляющих шумные публичные акции.

Одна из старейших групп DrinkOrDie до недавнего времени имела свой «официальный» сайт, где утверждалось, что ее основал москвич по кличке Deviator в 1993 г. В 1995 г. деятельность группы приобрела международную известность. Именно тогда входящие в нее хакеры распространили «пиратскую» версию операционной системы Windows 95 на две недели раньше ее официального выпуска. А пресечена деятельность группы была в 2002 г., когда ее лидера, ответственного, по утверждению следственных органов, за распространение в Интернете основной части «взломанного» программного обеспечения, приговорили к трем годам и восьми месяцам лишения свободы.

Как и во многих подобных группах, в DrinkOrDie существовало определенное разделение обязанностей. «Поставщики» (supplier), в число которых входили администраторы компьютерных сетей и студенты крупнейших американских университетов, доставали программы до их официального выхода, «кракеры» взламывали защиту, «курьеры» обеспечивали распространение «доработанных» программ. К 2000 г. DrinkOrDie превратилась в крупную международную организацию, имеющую представительства во многих странах мира и объединяющую большое число более мелких групп. По различным оценкам, в составе таких групп насчитывалось до полутора тысяч активных членов в 12 государствах. Лидеры организации проживали в США и Австралии. Участники групп, как правило, не получали доход от своей незаконной деятельности, в основном они стремились получить имидж «взломщика»-профессионала[158].

Типологизация личности компьютерного преступника возможна по различным основаниям. В. В. Лунев отмечает, что мотивационная сфера является центром внутренней структуры личности, интегрирующем ее активность[159]. Под мотивационной сферой личности понимается вся совокупность ее мотивов, которые формируются и развиваются в течение ее жизни»[160]. Нельзя забывать и о том, что наличие или отсутствие мотива к совершению определенных дейст-

---

[158] См.: Осипенко А.Л. Указ. соч. С. 160-163.
[159] Лунев В.В. Мотивация преступного поведения. М., 1991. С. 107.
[160] Ломов Б.Ф. Методологические и теоретические проблемы психологии. М., 1999. С. 204.

вий имеет значение в доказывании виновности лица, в определении степени общественной опасности виновного и его деяний, а характер побуждений нередко выступает обстоятельством, отягчающим или смягчающим ответственность.

Основываясь на анализе результатов зарубежных и отечественных исследований всех компьютерных преступников по особенностям мотивации преступного поведения можно классифицировать следующим образом. Наиболее характерными мотивами лиц, совершающих преступления, связанные с незаконным оборотом вредоносных компьютерных программ, можно считать: корыстные; хулиганские; политические; игровые, исследовательский интерес; потребность в самоутверждении; месть; мотивы, связанные с психическими отклонениями. При наличии достаточно широкого спектра мотивов, наиболее распространенными являются корыстные, игровые, связанные со стремлением к самоутверждению.

Необходимо отметить, что масштабы корыстных преступлений против собственности и объемы причиняемого ущерба от преступлений в сфере компьютерной информации год от года увеличиваются. Все чаще заявляют о себе, в частности, вымогатели, промышляющие в компьютерных сетях. Излюбленным методом преступной деятельности таких лиц является умышленное заражения вирусом компьютерных сетей с последующим навязыванием услуг по их восстановлению за денежное вознаграждение. При этом группа вымогателей может разделить свои обязанности – внедряют вирус одни лица, а восстанавливают сети другие лица.

Как показывает анализ, корыстный тип компьютерного преступника – это, как правило, лицо, достигшее 25-летия. Для компьютерных преступников младшего возраста характерно совершение преступлений, связанных с незаконным оборотом вредоносных компьютерных программ бескорыстного характера, в основном из любопытства, с целью самоутверждения, ради удовольствия, игры.

Для другой группы компьютерных преступников доминирующими являются мотивы связанные со стремлением к самоутверждению. Представители этой группы зачастую пытаются получить известность путем создания вредоносных программ. Можно считать, что мотивом преступных действий для представителей названного типа преступников является утверждение себя в жизни через приобретение или сохранение определенного социального статуса. Для представителей этого типа характерны честолюбие, целеустремленность, решительность, стремление к лидерству. Они отличаются хорошей приспособляемостью, так как ориентируются в социальных нормах и требованиях, имеют социальный опыт и могут контролировать своё поведение.

Криминологи отмечают частое сочетание мотивов корысти и утверждения себя в жизни[161]. Учитывая возрастные особенности лиц, совершающих преступления исследуемой категории, такое сочетание представляется вполне закономерным.

---

[161] См.: Антонян Ю.М. Психология преступника и расследования преступлений / Ю.М. Антонян, М.И. Еникеев, В.Е. Эминов. М., 1996. С. 168.

Нередко взломы, особенно направленные на блокирование работы систем, связаны и с различного рода деструктивными мотивами. Такие мотивы поведения подростков известны давно и проявляются не только по отношению к компьютерам. Очевидно, определенная часть молодежи пытается реализовать свои наклонности к вандализму в киберпространстве, где все представляется не настолько серьезным, как в реальной жизни, и при этом велика вероятность остаться безнаказанным. Между тем, исследователи полагают, что даже те противоправные деяния, которые принято объяснять хулиганскими деструктивными побуждениями, на самом деле связаны со стремлением подтвердить себя в качестве социального и биологического существа, т. е. все с тем же мотивом утверждения, основанным на потребности ощущать себя источником изменений в окружающем мире[162]. Естественно, такая мотивация молодых людей может изменяться по мере взросления.

Среди типов компьютерных преступников, для которых корыстные мотивы не являются ведущими, можно выделить игровой тип. Поведение этого типа преступников детерминируется потребностью к игре, риску, испытать острые ощущения, включиться в эмоционально возбуждающие ситуации. Они получают психологическое удовлетворение в самом процессе преступной деятельности. Вступая в интеллектуальное противоборство с системами сетевой безопасности, подобные индивиды воспринимают свои действия как проверку своих навыков и сообразительности, способности адекватно оценивать ситуацию и быстро принимать решения.

Для игрового типа компьютерных преступников характерно отсутствие серьезных познаний в области программирования и компьютерной техники. Данная категория преступников имеет, как правило, лишь некоторые пользовательские навыки работы с компьютером. Их действия направлены на уничтожение, блокирование, модификацию, копирование ничем не защищенной информации, создание вредоносных программ. К игровому типу часто относятся несовершеннолетние лица, главным образом, школьники. Примечательно, что, по мнению специалистов, пик активности вредоносных программ обычно приходится на осень и на период после зимних праздников. Именно тогда заканчиваются каникулы, во время которых юные программисты получают возможность практиковаться в создании подобных программ.

В рамках игрового типа особо можно выделить группы хакеров, которые осуществляют хакерские акции с целью испытания своих интеллектуальных и профессиональных способностей, а также тех, кто играет ради удовольствия, из увлечения, скуки.

Следующий мотивационный тип компьютерных преступников составляют лица, которые руководствуются соображениями мести. Этих людей нельзя подвести под общие рамки вирусописателей, так как у каждого их них своя мораль. Их не интересуют закон и беспокойство о том ущербе, который может понести пострадавший. У каждого из них есть своя персональная цель. Их задача – нанести максимальный урон.

---

[162] См.: Антонян Ю.М. Указ. соч. С. 168.

Кроме указанных, к числу потенциальных преступников можно отнести лиц, страдающих новым видом психических заболеваний - информационными болезнями, или компьютерными фобиями. Эта категория заболеваний связана с нарушениями информационного режима человека под воздействием внешних или внутренних дестабилизирующих факторов как врожденного, так и приобретенного свойства, которые вызываются информационным голодом, информационными перегрузками, неплановыми переключениями с одного информационного процесса на другой, информационным шумом и др.

В отдельных случаях исследователи предполагают даже наличие определенной психологической зависимости субъекта, выражающейся в навязчивой потребности осуществлять взломы компьютерных систем. В 1993 г. в Англии на судебном слушании было признано, что обвиняемый в сетевых проникновениях Бедворт страдает подобной зависимостью. Аналогичная потребность наблюдалась и у К. Митника, которого ФБР включило в список 10 наиболее опасных преступников США. Судья, выносивший приговор Митнику, объявил, что «видит определенную параллель между его пристрастием к взлому компьютерных сетей и влечением других людей к наркотикам»[163]. Сам Митник утверждал, что он мог бы стать миллионером, продавая полученные секретные сведения, однако не использовал эти возможности, а лишь «развлекался», взламывая чужую защиту.

По нашему мнению, в зависимости от характера совершаемых деяний, составляющих объективную сторону преступления, предусмотренного ст. 273 УК РФ, из совокупности всех преступников, осуществляющих незаконный оборот вредоносных компьютерных программ можно выделить: создателей вредоносных программ, пользователей и распространителей. В основе выделения этих групп лежат значительные различия в профессиональных навыках лиц, осуществляющих эти деяния.

К группе создателей вредоносных программ мы относим лиц, создающих подобные программы, в том числе и путем внесения изменений в уже существующие программы. В зависимости от уровня профессиональной подготовки среди создателей целесообразно выделить два типа: профессиональный и начинающий.

К преступникам профессионального типа относятся в основном лица мужского пола в возрасте от 25 до 35 лет с высшим техническим образованием, продолжительным опытом работы в области информационных технологий и высокой профессиональной подготовкой. Такие лица сразу оценивают свои возможности по извлечению прибыли из своей деятельности. И не получая соответствующего своим способностям вознаграждения, переходят в «теневую область». Преступники профессионального типа с некоторым превосходством относятся к требованиям норм права. Они практически не досягаемы для правоохранительных органов.

Преступниками начинающего типа являются лица в возрасте до 25 лет, в подавляющем большинстве мужского пола. Образование среднее, среднее спе-

[163] Зубков А. Кевин Митник вышел на свободу // Мир Internet. 2000. №3. С. 48-49.

циальное, высшее, неоконченное высшее. Все ступени образования, так или иначе, связаны с технологией, в основном, компьютерной. Преступную деятельность начинают достаточно рано. Пишут вредоносные программы в основном для «пробы пера». Для этих лиц характерны мотивы связанные со стремлением к самоутверждению и игровые мотивы.

К пользователям мы относим лиц, приобретающих вредоносные программы (например, копируя в память компьютера через сеть, получая программы вместе с машинным носителем в результате акта дарения, мены, купли-продажи, дачи взаймы и т.д.) и использующих их по прямому назначению. Образование среднее, среднее специальное, высшее, неоконченное высшее. Чаще это лица мужского пола, хотя встречаются и женщины. Пользователи слабо разбираются в основах программирования, используют готовые программные средства, часто даже не понимая принципов их действия, однако могут причинить значительный ущерб. Основой мотивации таких преступников чаще всего является любопытство, месть, хулиганские, игровые мотивы.

Распространители вредоносных программ – лица, предоставляющие доступ к вредоносным программам сетевым или любым другим способом. Чаще всего это мужчины в возрасте до 30 лет, имеющие среднее, среднее специальное, высшее образование, не всегда техническое, и не очень глубокие знания в области компьютерных технологий. В большинстве случаев такие лица руководствуются корыстными мотивами. Статистика показывает, что наибольшее количество дел, квалифицированных по ст. 273 УК, составляют дела, в которых объективной стороной преступления является распространение вредоносных программ путем продажи через розничную сеть лазерных компакт-дисков, содержащих такие программы. Можно утверждать, что применение ст. 273 УК РФ к такому виду преступных деяний наиболее эффективно демонстрирует превентивную силу закона.

Итак, изучение особенностей лиц, совершающих преступления, является важным условием правильной организации борьбы с определенным видом преступной деятельности. Для преступлений, связанных с незаконным оборотом вредоносных программ, изучение личности преступника приобретает особую актуальность, так как в данном случае речь идет о субъектах, которые до недавнего времени не попадали в поле зрения правоохранительных органов.

Типологизация личности компьютерного преступника может проводиться по различным основаниям (например, по особенностям мотивации, по уровню подготовленности, преступной специализации и т.д.). Такие сведения позволяют наиболее полно составить обобщенный криминологический портрет субъекта, совершающего преступления, связанные с незаконным оборотом вредоносных программ.

При криминологической характеристике личности преступников, совершающих преступления, связанные с незаконным оборотом вредоносных программ, считаем, что их можно классифицировать в зависимости от характера совершаемых деяний и различиях в профессиональных навыках этих лиц на три группы: создателей, пользователей и распространителей. В сферу действия уголовного закона в основном попадают распространители. Это, как

правило, мужчины в возрасте до 30 лет, имеющие не глубокие знания в области компьютерных технологий и, в большинстве случаев, руководствующиеся корыстными мотивами.

3.3. Актуальные направления предупреждения преступности, связанной с незаконным оборотом вредоносных компьютерных программ

В Концепции национальной безопасности Российской Федерации[164] отмечается, что серьезную угрозу для национальной безопасности России представляет рост масштабов преступности, в первую очередь организованных ее форм. Несомненно, внедрение и использование автоматизированных информационных систем остро ставит вопрос обеспечения информационной безопасности личности, общества, государства и защиты информации, обрабатываемой в информационных системах и передаваемой по каналам связи. Особенно актуальна эта проблема в связи с созданием общефедеральных систем и баз данных, таких как государственный реестр населения, база налогоплательщиков, государственная автоматизированная система «Выборы», единая автоматизированная система управления на железнодорожном транспорте и др.

Степень негативного воздействия указанных обстоятельств на состояние безопасности страны увеличивает «отсутствие эффективной системы социальной профилактики правонарушений, недостаточная правовая и материально-техническая обеспеченность деятельности по предупреждению преступности, правовой нигилизм, отток из органов обеспечения правопорядка квалифицированных кадров…»[165]. Как видим, на первое место среди факторов усугубления отрицательного влияния различных угроз на безопасность личности, общества и государства Концепция выдвигает отсутствие эффективной системы профилактики правонарушений.

И действительно, ставшее уже банальным за много веков утверждение о том, что болезнь легче предотвратить, чем лечить, не теряет своей актуальности и по сей день. Преодолевать и сдерживать преступность и иные формы девиантного поведения, изобилующие в обществе, лишь путем установления правовых запретов и применения мер государственного принуждения невозможно. Эти положения постулировали еще просветители XVIII в., хотя и задолго до них древнегреческие философы Аристотель и Платон высказывали некоторые идеи относительно предупреждения преступного поведения.

Все сказанное имеет непосредственное отношение к той форме преступности и той разновидности девиантного поведения, которая является предметом нашего рассмотрения, т.е. к незаконному обороту вредоносных компьютерных программ. Сдержать распространение вредоносных программ и хоть в какой-то мере сократить их уровень возможно лишь путем осуществления широкомасштабной научно обоснованной программы предупреждения, к разработке и реализации которой должны быть привлечены самые различные органы и организации, а также специалисты многих отраслей знаний, в частности, юристы, технические специалисты, педагоги, социологи.

Структура преступности, связанной с незаконным оборотом вредоносных программ может быть представлена следующим образом.

---

[164] Утверждена Указом Президента РФ от 17 декабря 1997 г. № 1300 (в ред. Указа Президента РФ от 10 января 2000 г. №24) // СЗ РФ. 2000. №2. Ст. 170.

[165] Там же. Разд. III.

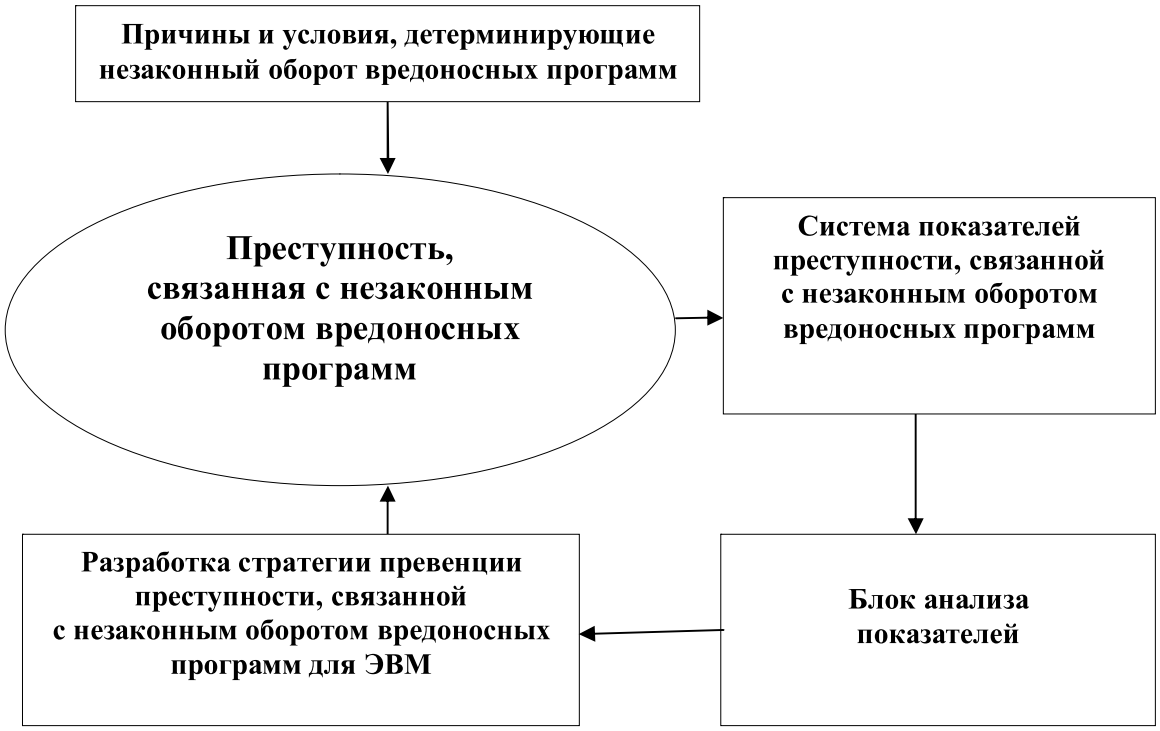

Рисунок 1. Общая структура преступности, связанной с незаконным оборотом вредоносных компьютерных программ.

Компонентами данной структуры являются: преступность, связанная с незаконным оборотом вредоносных программ, комплекс причин и условий, детерминирующих данный вид преступности, выходные показатели, характеризующие состояние этого вида преступности на современном этапе, аналитический блок в цепи обратной связи, осуществляющий сбор и обобщение выходных показателей и выработку на этой основе превентивных стратегий. Особенности перечисленных компонентов были рассмотрены нами в предыдущих разделах данного исследования. В этом разделе речь пойдет о выработке стратегии превенции преступности, связанной с незаконным оборотом вредоносных компьютерных программ.

Предупреждение преступности, связанной с незаконным оборотом вредоносных компьютерных программ, – это целенаправленное воздействие государства, общества, физических и юридических лиц на процессы детерминации и причинности данного вида преступности в целях недопущения вовлечения в преступность новых лиц, совершения новых криминальных деяний в сфере компьютерной информации, расширении криминализации общественных отношений[166]. По мнению специалистов, результаты предупредительной работы при ее правильной организации и целенаправленном осуществлении, оказывают существенное положительное влияние на уровень, структуру и динамику преступности, обеспечивают последовательное снижение количества совершаемых преступлений.

[166] Криминология: Учебник для вузов / Под ред. А.И. Долговой. С. 435.

Сложность предупреждения преступлений определяет многообразие видов этой деятельности, которые выделяются в зависимости от различных оснований. Так, по характеру (опосредованному или непосредственному) предупреждения преступлений выделены его общесоциальный и специально-криминологический виды[167].

Общесоциальное предупреждение преступлений характеризуется тем, что составляющие его меры являются необходимым элементом социально-экономической деятельности, устранения недостатков в политической, социальной, нравственно-психологической и духовной сферах общества. Они, как правило, связаны с улучшением материального благосостояния граждан, условий их труда и отдыха, укреплением дисциплины и организованности, а также с другими позитивными изменениями в обществе. Направленные на решение указанных задач, эти меры попутно устраняют негативные процессы и явления, выполняя при этом опосредованно функцию предупреждения преступлений. Мероприятия рассматриваемого уровня оказывают также опосредованное воздействие на весь механизм поведения личности, на причины конфликтов между личностью и обществом, личностью и государством, лежащие в основе формирования той или иной разновидности девиантного поведения. Это воздействие личность претерпевает перманентно в течение всей своей жизни, с момента начала формирования. Осуществление этих мероприятий не имеет перед собой единственной непосредственной цели – предупредить антиобщественное поведение, но, как мы уже отмечали, опосредованное воздействие на проявления личности в обществе оно имеет колоссальное, если не сказать определяющее.

В Концепции национальной безопасности РФ названы магистральные направления решения указанных проблем. В сфере экономики – это принятие необходимых мер по преодолению последствий экономического кризиса, переход к экономическому росту, подъем экономики страны, проведение независимого и социально ориентированного экономического курса, подъем благосостояния граждан и др.

В социальной сфере – нивелирование процесса расслоения общества на узкий круг богатых и преобладающую массу малообеспеченных граждан, снижение удельного веса населения, живущего за чертой бедности, сокращение уровня безработицы, укрепление фундаментальной ячейки общества – семьи. Сюда же следует отнести такие меры, как воспитание законопослушных граждан, создание необходимых условий для осуществления творческой деятельности и функционирования учреждений культуры.

В области политики – совершенствование системы государственной власти России, законодательства РФ, формирование гармоничных межнациональных отношений, сохранение социально-политической стабильности, формирование оптимальных механизмов распределения в обществе, укрепление правопорядка, обеспечение эффективной защиты личности, общества и государства от преступных посягательств, усовершенствование мер административного,

---

[167] Криминология: Учебник для вузов / Под ред. проф. В.Д. Малкова. 2-е изд. М.: ЗАО «Юстицинформ», 2006. С. 120.

гражданского и уголовно-правового воздействия на нарушителей закона, укрепление системы правоохранительных органов, создание условий для их эффективной деятельности.

В области идеологии – духовное обновление общества, укрепление нравственного и творческого потенциала населения, обеспечение защиты культурного, духовно-нравственного наследия, исторических традиций и норм общественной жизни, формирование государственной политики в области духовного и нравственного воспитания населения.

Следует признать, что в настоящее время общесоциальный уровень в значительной мере ослаблен из-за наличия различных социально-экономических негативных процессов, осложняющих жизнеобеспеченность членов нашего общества.

Специально-криминологическое предупреждение преступлений характеризуется совокупностью мер, специально направленных на устранение причин преступности или конкретных преступных проявлений. Масштаб их применения, как правило, намного меньше, чем у общесоциальных мер, хотя в некоторых случаях он приобретает значительные размеры. Объектами такого предупреждения являются как преступность в целом, так и ее виды, а также отдельные преступления.

Специально-криминологическое предупреждение преступлений — это социальный процесс, основой которого является применение отвечающих требованиям общественной морали и законности специальных методов и приемов, знаний и навыков регулирования социальных отношений в целях ликвидации тех их отрицательных последствий, которые могут вызвать совершение преступлений. Специально-криминологическое предупреждение называется таковым не только потому, что оно направлено на достижение указанных целей, но и потому, что требует специальных криминологических знаний, которые необходимы и при разработке комплексных планов и целевых программ, и при выработке и реализации мер предупреждения отдельных видов преступлений и т.д.

Безусловно, предупреждение преступлений, связанных с незаконным оборотом вредоносных компьютерных программ, предусматривает необычайно сложный комплекс разнообразных мероприятий — от принятия новых законов до поиска технических решений по защите сетевых объектов. Разнообразные мероприятия, входящие в этот комплекс направлены на повышение трудности совершения преступления, повышение риска при совершении преступления, уменьшение выгоды от совершения преступления[168].

На основе данных, полученных в ходе анализа отечественной и зарубежной специальной литературы и публикаций в периодической печати по вопросам теории и практики борьбы с преступностью в сфере компьютерной информации, а также с преступностью, связанной с незаконным оборотом вредоносных компьютерных программ, нами выделяются три основные группы мер предупреждения компьютерных преступлений, составляющих в своей совокупно-

[168] См.: Кудрявцев В.Н. Генезис преступления: Опыт криминологического моделирования: Учебное пособие. М., 1998. С. 136.

сти целостную систему борьбы с этим социально опасным явлением, а именно: правовые, организационные и технические.

Первая группа предполагает совершенствование правовых механизмов: улучшение правовой базы, четкое определение составов соответствующих преступлений, обеспечение их эффективного обнаружения, расследования и уголовного преследования. Вторая предусматривает главным образом предотвращение преступлений за счет осуществления мероприятий организационного характера: осуществление кадровой политики с целью обеспечения компьютерной безопасности, разработка комплексного плана защиты информации; определение приоритетных направлений защиты информации в соответствии со спецификой деятельности организации; определение ответственности сотрудников организации за безопасность информации в пределах установленной им компетенции путем заключения соответствующих договоров между сотрудниками и администрацией предприятия, учреждения, организации и т.п. Третья предусматривает совершенствование технических средств защиты: создание аппаратного и программного обеспечения вычислительных систем, которые препятствуют или делают трудноосуществимой преступную деятельность, разработка вопросов технической защиты компьютерных залов и компьютерного оборудования.

Следует отметить, что в последнее время роль правового решения проблем обеспечения безопасности мирового информационного пространства становится все более заметной. Практика показала полную несостоятельность подхода, при котором считалось, что безопасность глобальных сетей может быть обеспечена только за счет морально-этического воздействия на потенциальных нарушителей и осуществления защитных организационно-технических мероприятий (в основном разработки и установки специализированных аппаратно-программных комплексов на защищаемых объектах). В этом отношении достаточно упомянуть, что в начале 2000 г. взлому подвергся даже сайт компании RSA Security Inc., которая является одним из признанных мировых лидеров в разработке систем защиты для электронной коммерции[169].

Отечественное законодательство относительно недавно встало на путь борьбы с преступностью в сфере компьютерной информации, с опозданием от западных стран на двадцать с лишним лет. Как следствие, если в США на сегодня действуют более 2000 законов и подзаконных актов, в той или иной мере касающихся подобных преступлений и связанных с ними явлений, то в России их число в районе десяти[170]. Как было отмечено нами ранее в п.п. 1.1 и 2.2, отечественное законодательство является явно недостаточным и несоответствующим сложившейся в стране ситуации с обеспечением информационной безопасности. 91% опрошенных нами респондентов в ходе проведения социологического исследования, на вопрос «Считаете ли Вы, что для эффективной борьбы с преступлениями в сфере компьютерной информации создана необходимая законода-

---

[169] Осипенко А.Л. Указ. соч. С. 406.

[170] См.: Згадзай О.Э. Преступления в сфере компьютерной информации: Аналитический обзор / О.Э. Згадзай, С.Я. Казанцев, Р.М. Оболенский. Казань, 2003. С. 63.

тельная база?», ответили: «Нет, законодательная база нуждается в серьезной доработке».

Специалисты отмечают фрагментарность, декларативность и определенную противоречивость действующего законодательства в сфере информационной безопасности. Отдельные нормативно-правовые акты вполне очевидно создавались без необходимых консультаций с техническими специалистами, в связи с чем, закрепленные в них правовые положения не работоспособны на практике[171].

Среди недостатков необходимо отметить сложность конструкций правовых норм, наличие в них технических понятий и специальных терминов; мягкость санкций ст. 272-274 УК; отсутствие обобщений следственной и судебной практики, которые могли бы быть ориентиром в правильной квалификации преступлений.

В гл. 28 УК РФ говорится об общественно опасных деяниях в сфере компьютерной информации. Безопасность этой сферы является объектом уголовно-правовой защиты. Однако определения сферы компьютерной информации нет ни в одном нормативном акте Российской Федерации. Нет определений и ряда других понятий, используемых в диспозициях ст. 272-274 УК РФ и имеющих значение для квалификации.

Кроме того, многие авторы указывают на то, что целый ряд реально существующих общественно опасных деяний невозможно квалифицировать по имеющемуся УК. В частности, в исчерпывающий перечень деяний ст. 272 УК РФ, являющихся результатом неправомерного доступа к компьютерной информации, не вошло простое, распространенное и опасное — чтение информации. Ответственность по данной статье наступает лишь в том случае, если этот доступ повлек «уничтожение, блокирование, модификацию либо копирование информации». Таким образом, чтение информации, охраняемой законом, преступлением не является[172].

Далее, рост преступлений в сфере компьютерной информации находится в прямой зависимости от постоянного развития компьютерных технологий и новых способов распространения информации с использованием возможностей глобальных компьютерных сетей. Остановить лавину преступлений в сфере высоких технологий возможно лишь при совершенствовании правового поля в деле правомерного использования информационного пространства, а именно в мировой компьютерной сети Интернет. Таким образом, важным направлением борьбы с преступностью, связанной с незаконным оборотом вредоносных компьютерных программ, должно стать становление и развитие правового фундамента в сфере Интернета путем принятия соответствующего закона.

К правовому обеспечению относится и составление договоров на проведение работ и на оказание информационных услуг. Здесь правовая гарантия предусматривается определенными условиями ответственности за нарушение сто-

---

[171] См.: Дамаскин О.В. Актуальные вопросы законодательного обеспечения национальной безопасности в условиях глобализации // Системы безопасности. 2003. № 3. С. 90-91.

[172] Быков В. Совершенствование уголовной ответственности за преступления, сопряженные с компьютерными технологиями / В. Быков, А. Нехорошев, В. Черкасов // Уголовное право. 2003. № 3. С. 10.

ронами принятых обязательств (помимо возмещения убытков, возможны штрафные санкции).

В условиях неразвитого государственного правового механизма обеспечения безопасности компьютерных сетей серьезное значение приобретают документы предприятия, регулирующие отношения с государством и с коллективом сотрудников на правовой основе. К таким основополагающим документам, которые также играют важную роль в обеспечении безопасности, можно отнести: устав предприятия (фирмы, банка), закрепляющий условия обеспечения безопасности деятельности и защиты информации; коллективный договор; трудовые договоры с сотрудниками предприятия, содержащие требования по обеспечению защиты сведений, составляющих коммерческую тайну и др.; правила внутреннего трудового распорядка рабочих и служащих; должностные обязанности руководителей, специалистов и обслуживающего персонала.

Законотворчество в сфере компьютерной информации должно быть направлено на развитие межгосударственного и внутригосударственного законодательства, регулирующего обмен информацией. Межгосударственное информационное законодательство включает в себя двусторонние и многосторонние соглашения с государствами ближнего и дальнего зарубежья. Разработка и подписание таких соглашений обеспечат безопасную интеграцию России в мировое информационное пространство. Внутригосударственное законотворчество заключается в создании информационного законодательства, отвечающего всем требованиям современности и адаптированного к нормам международного права.

Сегодня становится все более очевидным, что единственный путь для гармонизации правового регулирования в глобальных сетях связан с унификацией законодательного регулирования за счет выработки международными организациями взаимоприемлемых принципов. В последнее время большинство государств, в том числе и Россия, проявляют заметную активность в поиске таких принципов[173]. Среди наиболее важных документов в этой сфере особое место занимает Конвенция по борьбе с киберпреступностью[174], которую в результате глубокого и всестороннего изучения проблемы принял Совет Европы. Конвенцию подписали представители 30 стран (26 европейских государств, США, Канада, Япония, ЮАР). В 2005 году было принято Распоряжение Президента РФ № 557-рп «О подписании Конвенции о киберпреступности», в котором МИД РФ поручается подписать данную Конвенцию, сопроводив подписание заявлением, в котором Россия обязуется «определиться в вопросе о своем участии в Конвенции при условии возможного пересмотра положений пункта «b» статьи 32 Конвенции». По мнению российской стороны, этот пункт дает возможность такого толкования ряда положений преамбулы Конвенции, которое может «нанести ущерб суверенитету и национальной безопасности госу-

---

[173] См.: Горяинов К.К. Транснациональная преступность / К.К. Горяинов, А.П. Исиченко, Л.В. Кондратюк. М., 1997. С. 254-251.

[174] Неофициальный перевод текста Конвенции см.: Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М., 2002. С. 375-414.

дарств-участников, правам и законным интересам их граждан и юридических лиц»[175].

Значение принятия Конвенции необычайно велико. Этот документ стал первым международным договором такого уровня, регулирующим правовые процедурные аспекты борьбы с киберпреступностью. Он четко определяет, в каких направлениях должны прилагаться основные усилия на национальном и международном уровнях[176].

Кроме того, в 1997 году было заключено Соглашение между правительством России и правительством Республики Белоруссия о сотрудничестве в области защиты информации. В целях реализации этого Соглашения его стороны договорились обмениваться опытом работы по вопросам защиты информации, при необходимости проводя консультации и создавая рабочие группы.

В 2001 году представителями ряда стран-участниц СНГ было подписано Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации. Согласно этому документу в качестве уголовно наказуемых (в рамках национального законодательства) признаются следующие деяния: осуществление неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети; создание, использование или распространение вредоносных программ; нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред или тяжкие последствия; незаконное использование программ для ЭВМ и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный вред[177].

Кроме того, государствами-членами СНГ предпринимаются активные усилия в направлении унификации национального законодательства. Например, весьма тщательно прописаны пути регламентации вопросов уголовной ответственности за преступления в сфере компьютерной информации в Модельном уголовном кодексе для стран-участников СНГ, принятом в 1996 на пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ. В соответствии с нормами раздела 12 «Преступления против информационной безопасности» наказуемы: несанкционированный доступ к компьютерной информации, модификация компьютерной информации, компьютерный саботаж, неправомерное завладение компьютерной информацией, изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети, разработка, использование и распространение вредоносных

---

[175] Собрание законодательства РФ. 2005. № 47. Ст. 4929.

[176] См. подробнее: Hammond A. The 2001 Council of Europe Convention on cyber-crime: an efficient tool to fight crime in cyber-space? Santa Clara University. Cedric J. Magnin. June, 2001. 112 p.

[177] См. подробнее: Ястребов Д.А. Институт уголовной ответственности в сфере компьютерной информации (опыт международно-правового сравнительного анализа) // Государство и право. 2005. № 1. С. 61-63.

программ, нарушение правил эксплуатации компьютерной системы или сети. Кодекс также предусматривает ответственность за совершение преступлений, связанных с незаконным использованием компьютеров или компьютерной информации. Установлена уголовная ответственность за: хищение, совершенное путем использования компьютерной техники; причинение имущественного ущерба путем обмана, злоупотребления доверием или модификации компьютерной информации; незаконное получение информации, составляющей коммерческую или банковскую тайну путем перехвата в средствах связи, незаконного проникновения в компьютерную систему или сеть, использования специальных технических средств; нарушение правил обращения с содержащими государственную тайну документами или компьютерной информацией.

Однако практически ни одно из государств-членов СНГ во внутригосударственном законодательстве в полной мере не реализовало рекомендации Модельного кодекса, что привело к тому, что нормы действующих УК стран СНГ не охватывают всего круга противоправных деяний, совершаемых в сфере компьютерной информации, что не способствует интересам защиты личности, общества и государства от таких преступлений.

Между тем общеизвестно, что одними правовыми мерами сдерживания не всегда удается достичь желаемого результата в деле предупреждения преступлений. Тогда следующим этапом становится применение мер организационного и технического характера для защиты компьютерной информации от противоправных посягательств на нее. Эти меры могут играть серьезную общепрофилактическую роль в борьбе с преступлениями, связанными с незаконным оборотом вредоносных компьютерных программ, при их умелом и комплексном использовании.

Рассматривая меры по обеспечению защищенности компьютерной информации следует начать с того, что компьютерные системы характеризуются уязвимостью. По мнению специалистов, использование постоянных, не развивающихся механизмов защиты опасно, и для этого есть несколько причин. Одна из них – развитие сети. Ведь защитные свойства электронных систем безопасности во многом зависят от конфигурации сети и используемых в ней программ. Даже если не менять топологию сети, все равно придется когда-нибудь использовать новые версии ранее установленных продуктов. И может случиться так, что новые возможности этого продукта пробьют брешь в защите.

Кроме того, нельзя забывать о развитии и совершенствовании средств нападения. Техника так быстро меняется, что трудно определить, какое новое устройство или программное обеспечение, используемое для нападения, может обмануть защиту.

Вместе с тем отсутствие абсолютной защиты не значит, что следует совсем отказаться от применения мер защиты. Чем уязвимее система, тем вероятнее успех вторжения в нее, ибо атака на компьютерную систему – это не что иное, как поиск и использование злоумышленниками уязвимости системы. Конечно, обеспечение безопасности информации – дело дорогостоящее. Но вместе с тем надо иметь в виду, что дорогостоящим его делают не столько затраты на закупку или установку различных технических или программных средств,

сколько то, что трудно квалифицированно определить границы разумной безопасности и соответствующего поддержания системы в работающем состоянии. С другой стороны, как показывает опыт и статистика стоимость восстановления информации и ИТ-ресурсов после атак намного превосходит стоимость даже самых дорогих средств защиты.

Исходя из изложенного, можно заключить, что одно из важнейших мест в комплексе необходимых мер по защите компьютерной информации должны занимать меры технического характера и, прежде всего, физические, программно-аппаратные и криптографические.

Физические средства включают в себя различные инженерные средства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и защищающие персонал, материальные средства и финансы, информацию от противоправных действий.

К программно-аппаратным средствам относятся приборы, устройства, приспособления и другие технические решения, а также специальные программы, программные комплексы и системы защиты информации, используемые в интересах обеспечения безопасности.

В практике деятельности любой организации в целях предупреждений хакерских угроз рекомендуется использовать различную аппаратуру и, прежде всего, межсетевые экраны, системы обнаружения атак, системы шифрования трафика, системы контроля «мобильного кода» (Java, ActiveX) и т.п.

Существует мнение, согласно которому никакие средства не могут спасти от хакерской угрозы. Это касается и программно-аппаратных средств защиты. Однако вопрос в том, чтобы сделать усилия хакеров если не бесполезными, то, во всяком случае, настолько затратными, чтобы они потеряли всякий интерес к атакуемой сети.

Основные направления использования криптографических методов — это передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

При рассмотрении вопросов, касающихся программной защиты информационных ресурсов, специалистами особо выделяется проблема их защиты от вредоносных компьютерных программ. По оценкам многих специалистов, от решения проблем борьбы с этим видом преступления в сфере компьютерной зависит не только надежность и бесперебойность функционирования компьютерных информационных систем, но и вообще сам факт и возможность их существования[178].

Для решения этой проблемы помимо организационно-правовых средств, необходимо активно использовать и специальные программные антивирусные средства защиты. В настоящее время разрабатываемые отечественные и зарубежные программные антивирусные средства позволяют с определенным успехом опознать зараженные и незараженные программные средства и их компо-

[178] См.: Черкасов В.Н. Теория и практика решения организационно-методических проблем борьбы с экономической преступностью в условиях применения компьютерных технологий. М., 1994. С. 45.

ненты, а также проконтролировать доступ к вычислительным ресурсам (данным, программам, оборудованию и т. д.).

По оценкам специалистов, существует уже достаточное количество различных антивирусных программных средств, позволяющих надежно защитить средства компьютерной техники от компьютерного вируса. Надежность этих средств составляет 97%. Но, тем не менее, всегда остаются те самые 3%, которыми и пользуются преступники для совершения компьютерных преступлений, ибо не существует абсолютно надежных средств защиты компьютерной техники от различного рода преступных посягательств.

Таким образом, как отмечалось нами, никакая технология не способна защитить от постоянно возникающих угроз, вместе с тем только создание комплексной системы защиты информации, учитывающей не только технические, но и организационные меры, о чем пойдет речь далее, сможет сделать компьютерную информацию недоступной для хакеров.

Интервьюирование сотрудников отдела «К» УВД Орловской области позволило сделать следующий вывод о том, что усиление борьбы с преступностью в сфере компьютерной информации во многом зависит от качественного разрешения следующих проблем:

- оснащение сотрудников подразделения необходимой материально-технической и методической базой;
- усиление взаимодействия аналогичных подразделений на региональном, всероссийском и международном уровнях;
- налаживание сотрудничества подразделений, осуществляющих борьбу с компьютерной преступностью и субъектами информационного оборота.

Организация противодействия криминальным проявлениям в информационной сфере невозможна без привлечения к этой деятельности гражданских учреждений, промышленных предприятий и коммерческих компаний. Это обстоятельство обусловливается рядом причин.

Во-первых, большинство жертв подобных преступлений — коммерческие компании. Степень их доверия к представителям правоохранительных органов, готовность сотрудничать с ними в ходе следствия оказывают существенное влияние на эффективность борьбы с соответствующими преступлениями.

Во-вторых, сетевой администратор компании, подвергшейся нападению, становится ключевой фигурой для обеспечения успеха расследования, так как лишь он во всей полноте знает уникальную конфигурацию компьютерной системы и способен обнаружить критические данные, которые обеспечат необходимые доказательства противоправной деятельности.

В-третьих, предприятия, связанные с производством и обслуживанием вычислительной техники и программного обеспечения, способны оказать существенную помощь в проведении технических экспертиз. Для правоохранительных органов было бы экономически неоправданным содержать экспертов по всему разнообразию применяемых на практике операционных систем и сетевых конфигураций. Кроме того, часто возникает потребность в уникальных технических инструментальных средствах, разработка которых возможна исключительно при содействии специалистов указанных предприятий.

Одной из основных задач данного направления для нашей страны, безусловно, является создание в ведомственных учреждениях высшего профессионального образования современной кадровой, методической и материально-технической базы подготовки и переподготовки нужных специалистов. Система подготовки кадров должна подкрепляться научными исследованиями соответствующего профиля. Развитие подобной системы должно не только исходить из требований сегодняшнего дня, но и учитывать тенденции изменения преступности в будущем. Формирование кадрового ядра специализированных подразделений правоохранительных органов должно включать три важных направления: профессиональную подготовку, переподготовку и повышение квалификации их сотрудников. При этом особое внимание следует уделять последнему направлению: каждый работник, задействованный по рассматриваемому направлению, должен регулярно проходить обучение, с тем чтобы быть в курсе новаций в области технологий и сложившейся юридической практики.

Низкий уровень теоретической и практической подготовки сотрудников правоохранительных органов в рассматриваемой сфере специалисты связывают и со слабой обеспеченностью экспертными исследованиями соответствующего профиля, с отсутствием необходимой криминологически значимой информации о преступности в сфере компьютерной информации, которую получают в результате соответствующих исследований. Поэтому на начальном этапе крайне важно создать эффективную систему учета подобной преступности, статистической отчетности и разработать порядок аналитической деятельности органов, осуществляющих борьбу с этим общественно опасным явлением. Полученные данные в совокупности с другими сведениями могут быть положены в основу более полного и всестороннего анализа проявлений преступности в сфере компьютерной информации, специфики и детерминации, а также оценки предыдущего опыта борьбы с этим явлением. Важны прогноз развития такого вида преступности, планирование борьбы с ней с точным определением целей и задач этой деятельности. В этой связи представляется перспективной организация по примеру ФБР специализированных структур, занимающихся изучением проблем преступности в сфере компьютерной информации, разработкой стратегических и тактических подходов к раскрытию новых видов преступлений на основе научного комплексного изучения тенденций компьютерных криминальных процессов. Несомненную пользу могло бы принести создание центра анализа сетевых инцидентов, призванного осуществлять аналитическую и методическую деятельность, информирование общественности об угрозах сетевой безопасности и методах профилактики.

Не менее сложную проблему создает недостаточная оснащенность специализированных подразделений средствами вычислительной техники, специальными приборами и оборудованием. По мнению специалистов, даже в развитых государствах Запада правоохранительные органы слишком слабо оснащены технически для эффективного противостояния преступности. Для нашей же страны ситуацию с технической обеспеченностью правоохранительных структур можно считать исключительно трудной. Между тем от такой оснащенности зависит не только результативность проводимых расследований, но и, что не

менее важно, качество проводимых криминалистических экспертиз, связанных с анализом доказательств в электронном виде.

Эффективность научно-исследовательских изысканий, направленных на предупреждение компьютерной преступности, также во многом определяется уровнем применяемого оборудования. И, безусловно, техническое оснащение напрямую определяется финансовыми вложениями. В этом отношении российские правоохранительные органы существенно отстают от тех же США, где общий бюджет национальных программ, связанных с информационной безопасностью, за пять лет достиг 22 млрд. долл. В ноябре 2002 г. Конгресс США выделил 903 млн. долл. только для поддержки в ближайшее пятилетие образовательных программ и сотрудничества государственного и частного секторов в области борьбы с компьютерными преступлениями[179].

Правительства зарубежных стран каждый год увеличивают государственные ассигнования, создают специальные центры, использующие новейшую технику для выявления нарушителей и предотвращения очередной волны новых видов преступлений. Так, в США в целях борьбы с компьютерными вирусами в 1989 г. при национальной лаборатории в Ливерпуле был учрежден наблюдательный отдел по компьютерным инцидентам. Он оценивает масштабы бедствия, определяет меры по его ликвидации и предоставляет технические средства, для этого поиск и задержание виновных проводятся в тесном сотрудничестве с правоохранительными органами[180].

Также следует упомянуть созданную в 1988 году группу реагирования на компьютерные происшествия CERT (Computer Emergency Response Team), существующую на средства Министерства обороны США, официальное представительство которого было создано в 2002 г. и в России (Центр реагирования на компьютерные инциденты (www.cert.ru).

В качестве сдерживающего фактора роста преступности в сфере компьютерной информации нередко называется ужесточение соответствующего уголовного законодательства. В совокупности факторов, способных в настоящее время сыграть роль сдерживающих в рассматриваемой сфере, по нашему мнению, на первый план выходит формирование в целом у общественности, а особенно среди девиантных слоев «сетевого сообщества», убежденности в способности правоохранительных органов обеспечивать безопасность глобальных компьютерных сетей. Некоторые исследователи отмечают, что эффект сдерживания преступности от размера наказания заметно ниже, чем от вероятности наказания. Поэтому общество может выиграть от роста неотвратимости наказания, чем от простого увеличения его размера[181]. Потенциальный преступник должен осознавать высокую вероятность быть обнаруженным и понести наказание.

Уровень подобного осознания невероятно низок даже в Соединенных Штатах и, по-видимому, останется таковым в ближайшем будущем. По мнению

---

[179] См.: Осипенко А.Л. Указ. соч. С. 261.
[180] Гордиенко И. Стража на границе миров // Компьютера. 1999. 13 апр. С. 38.
[181] См. Андриенко Ю.В. Указ. соч. С. 194-220.

специалистов, это связано с тем, что правоохранительные органы испытывают серьезную нехватку ресурсов и подготовленных специалистов.

Между тем большинство хакеров полагают, что обладают достаточным уровнем квалификации для того, чтобы их противоправные действия в сети не были выявлены правоохранительными органами. В таких условиях даже самая общая осведомленность лиц, склонных к совершению таких преступлений, о наличии эффективных способов обнаружения их противоправной деятельности и возможности наблюдения за их криминальной активностью в сети со стороны правоохранительных органов создаст предпосылки, удерживающие часть из них от совершения преступлений.

В свете сказанного важным элементом профилактики становится проведение целевых мероприятий и распространение информации об успешной борьбе с преступностью в сфере компьютерной информации. Подобные материалы могут размещаться в средствах массовой информации, а также путем создания специализированных сайтов в сети Интернет.

Организационные меры также подразумевают регламентацию производственной деятельности и взаимоотношений исполнителей таким образом, что уничтожение, блокирование, модификация либо копирование компьютерной информации становятся невозможными или существенно затруднительным за счет деятельности специально создаваемых административных служб, в компетенцию которых входит организация всех мероприятий по информационной безопасности и защите информации.

Необходимость защиты от посягательств злоумышленников на служебные и информационные данные, а также своевременной реакции и оперативного восстановления поврежденных или несанкционированно измененных данных делает необходимым создавать в организациях, вступающих в сообщество пользователей глобальных и региональных корпоративных компьютерных сетей, фирмах специальные административные службы, штатная структура, численность и состав которых определяются реальными потребностями фирмы, степенью конфиденциальности ее информации и общим состоянием безопасности.

Сотрудникам такой службы следует решать множество задач. По мнению некоторых экспертов, первым шагом к решению защиты информации должно стать создание собственной концепции информационной безопасности организации, которая должна представлять собой систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности, основным принципом которой должно стать обеспечение необходимого уровня защищенности от возможных угроз при минимальной стоимости средств и систем защиты[182].

По мнению специалистов, чаще всего взломы и кражи становятся результатом небрежной кадровой политики фирмы. Особое внимания требует прием на работу системных администраторов, специалистов в области компьютерной техники, программирования и защиты компьютерной информации. Именно они

---

[182] См.: Вихорев С. Практические рекомендации по информационной безопасности / С. Вихорев, А. Ефимов // JetInfo. 1996. № 7. Т. 2. С. 42-48.

представляют собой одну из самых больших потенциальных угроз для безопасности организации[183].

Одной из важнейших мер по предупреждению преступлений, связанных с незаконным оборотом вредоносных компьютерных программ, является обучение персонала поведению, затрудняющему сетевое вторжение. Это вовсе не так просто, как кажется на первый взгляд. Необходимо вводить ограничения на использование Интернета. Причем пользователи часто не представляют, чем эти ограничения обусловлены, поэтому всячески пытаются нарушать существующие запреты. Тем более запреты не всегда могут или бывают четко сформулированы.

В плане предупреждения вирусных посягательств нельзя полагаться только на антивирусные программы. По мнению специалистов, необходимо предпринять следующие комплексные организационно-технические меры, которые могут быть сокращены или расширены по своему содержанию, исходя из каждой конкретной ситуации:

1. Информировать всех сотрудников учреждения, организации об опасности и возможном ущербе в случае совершения вирусного посягательства.

2. Не осуществлять неофициальные связи с другими организациями, связанные с обменом программных средств. Запретить сотрудникам приносить на рабочее место программные средства (ПС) «со стороны» для работы с ними на компьютерах, находящихся в учреждении, организации по месту работы сотрудника. В крайнем случае, для этих целей может быть создано специальное автономное рабочее место для тестирования таких ПС на предмет установления наличия или отсутствия в них средств вирусного характера. Должны использоваться только официально распространяемые ПС, содержащиеся на оттестированных и опломбированных носителях машинной информации.

3. Запретить сотрудникам использовать и хранить на носителях и в памяти компьютеров игры, являющиеся источником повышенной опасности для безопасности компьютерных систем. Если такое запрещение не может быть обеспечено; то создать специальное игровое место или общий игровой файл, постоянно контролируемый сотрудниками службы компьютерной безопасности и имеющий «иммунные» средства антивирусной защиты.

4. Предостеречь сотрудников организации от использования ПС и носителей машинной информации, имеющих происхождение из учебных заведений различного уровня и профиля. Тем более ставящих целью их использование в компьютерных системах организации, например, для выполнения работы личного характера в свободное от основной работы время. В крайнем случае производить такую работу на изолированных компьютерах или с соблюдением определенных мер антивирусной безопасности и с особым контролем.

5. Если в процессе работы возникнет необходимость в использовании сторонних информационных компьютерных сетей, то для этих целей необходимо в обязательном порядке выделить специальное стендовое оборудование с

---

[183] См. подробнее: Гаджиев М.С. Указ. соч. С. 136-139.

обязательной его изоляцией от остальных. Все файлы, поступающие из внешней компьютерной сети, должны обязательно проверяться (тестироваться).

6. Создать архив копий ПС, используемых в непосредственной работе организации (обязательно должны храниться копии операционных систем, используемых системных ПС, необходимых для восстановления нормального режима работы компьютерных систем и т.п.) с одновременным исключением несанкционированного доступа к этому архиву.

7. Регулярно просматривать хранимые в компьютерной системе ПС, создавать новые их архивные копии, архивные копии файлов с обновляемой информацией и, где это возможно, использовать защиту типа «только чтение» для предупреждения несанкционированных манипуляций с ценными данными.

8. Периодически (а в организациях, имеющих ярко выраженную денежно-финансовую и кредитную функцию, — к концу каждого рабочего дня) проводить ревизионную проверку контрольных сумм файлов, путем их сличения с эталоном, иногда хранящимся в зашифрованном либо архивированном виде с защитой «только чтение».

9. Использовать для нужд электронной почты отдельный стендовый компьютер или ввести специальный отчет. Запретить использование ПС, полученных по внешним каналам связи с помощью электронной почты и не прошедших специального тестирования.

10. Контролировать ведение журналов операторов ЭВМ (работы ЭВМ). В случае отсутствия соответствующей записи при наличии работающего сотрудника принимать дисциплинарные меры воздействия.

11. Установить системы защиты информации на особо важных компьютерах.

12. Периодически пересматривать и обновлять ПС и всю систему антивирусной защиты и правила обеспечения компьютерной безопасности.

13. Постоянно контролировать исполнение установленных правил обеспечения безопасности СКТ и применять меры дисциплинарного воздействия к лицам, сознательно или неоднократно нарушавшим их[184].

Следует иметь в виду, что защита информации — дело достаточно дорогое, поэтому одним из принципов построения системы защиты должно стать дифференцирование степени защиты по ее важности и ценности. Для этого следует определять перечень охраняемых сведений и градировать их по степени важности, от чего должна зависеть степень ее защиты.

Следует отметить, что достаточно часто потерпевшие сами создают условия для совершения преступлений, связанных с незаконным оборотом вредоносных компьютерных программ, которые при должной осмотрительности с их стороны, могли бы предотвратить. Поэтому повысить эффективность предупреждения преступлений позволяют и меры виктимологической профилактики, которая в рассматриваемом случае должна распространять свое влияние на потенциальных жертв подобных преступлений. Основной целью такой деятельности должны стать: формирование у населения понимания опасности и противо-

[184] См.: Вехов В.Б. Указ. соч. С. 83-85.

законности соответствующих деяний, повышение ответственности граждан при использовании сетей; обучение методам защиты и противодействия таким преступлениям (например, за счет разработки соответствующих рекомендаций); наконец, выявление слабых мест в защите информации и обеспечение на таких участках усиленного оперативного прикрытия со стороны правоохранительных органов, а также внесение в исполнительные органы власти обязательных для рассмотрения представлений и предложений об устранении обстоятельств, способствующих совершению правонарушений. При этом, естественно, специальные подразделения должны обращать внимание прежде всего на те криминогенные факторы, нейтрализация или устранение которых находятся в пределах их компетенции. В качестве специфических вариантов пресечения преступной деятельности в глобальных сетях правоохранительные органы могут применять блокирование конкретной сетевой рабочей станции (прерывание услуг связи) в порядке п. 1 ст. 15 Закона об ОРД при обнаружении угрозы совершения преступления с ее использованием, а также создание и размещение на специализированных сетевых сайтах списков с указанием адресов, с которых осуществлялись противоправные действия в глобальных сетях[185].

По мнению некоторых специалистов, повышение общего уровня грамотности в области информационной безопасности может дать больший результат, чем покупка дорогостоящего защитного оборудования. Персонал защищаемых объектов должен хорошо представлять источники опасности, что можно и чего нельзя делать в глобальных сетях, какие меры предпринять в случае обнаружения непосредственной угрозы. Большинство исследователей сходится на том, что публикация материалов о способах совершения преступлений в сфере компьютерной информации и методах их выявления, пресечения и раскрытия оказывает в целом позитивный эффект на криминальную ситуацию[186].

Министерство юстиции США поддерживает в Интернете сайт, призванный бороться с компьютерной преступностью (www.cybercrime.gov). Здесь публикуются правительственные пресс-релизы, тексты выступлений политиков и руководителей правоохранительных ведомств, результаты слушаний в Конгрессе и другие документы, затрагивающие проблемы борьбы с преступностью в глобальных компьютерных сетях. На сайте размещены все существующие нормативные акты, регламентирующие поведение граждан США в киберпространстве. Рассказано также о том, как своевременно и по какому адресу сообщить о подобном преступлении.

Пристальное внимание должно уделяться профилактике противоправной деятельности среди подростков. Подросток должен осознавать, что его действия причиняют вред конкретным людям, что они вызывают общественное неодобрение и что, наконец, за ними может последовать наказание. Правоохранительные органы должны прилагать усилия к разобщению выявленных молодежных групп, имеющих противоправные намерения, но еще не ставших на путь совершения преступлений.

---

[185] См.: Осипенко А.Л. Указ. соч. С. 419-420.

[186] См.: Линде С. Несанкционированный доступ – примеры вторжения // Открытые системы. 1996. № 4 (18). С. 28-30.

Специалисты считают необходимым ввести образовательные программы для подростков и их родителей с тем, чтобы разъяснить, что такое киберпреступления и какая ответственность наступает при их совершении. По их мнению, необходимо постоянно повышать информационную культуру всех категорий пользователей глобальных компьютерных сетей.

США уделяют большое внимание формированию «киберэтики» своих граждан. С этой целью развернута государственная программа обучения детей и молодежи основам правомерного поведения в Интернете. Цели программы состоят в том, чтобы дать обучаемым понимание потенциальных отрицательных последствий, возникающих при неправомерном употреблении сетевой среды; персональных опасностей, которые существуют в Интернете, и методов их предотвращения. Образовательная программа Cybercitizen Partnership преследует цель показать родителям и учителям, насколько важна сетевая безопасность, и помочь им правильно объяснить детям, к каким последствиям для них самих и для окружающих может привести «киберхулиганство»[187].

Общепризнано мнение о том, что предупреждение любого, в том числе и преступления, связанного с незаконным оборотом вредоносных компьютерных программ, должно носить комплексный характер и относиться к компетенции государственных органов, а не различных коммерческих охранных структур, что имеет пока место в нашей стране. Этому учит нас и опыт зарубежных государств, где уже с 60-х гг. (с момента совершения первого подобного преступления) стали серьезно заниматься этими проблемами на государственном уровне.

Таким образом, к настоящему моменту сложился достаточно широкий комплекс мер различного характера, способных оказывать сдерживающий эффект на совершение преступлений, связанных с незаконным оборотом вредоносных компьютерных программ. Результативность предупредительной деятельности правоохранительных органов в данной сфере во многом будет зависеть от их методичного, обоснованного и умелого применения. Все меры предупреждения таких преступлений будут эффективными только тогда, когда они будут использоваться комплексно. Использование одной какой-либо меры без других мер предупреждения не может принести желаемого результата.

Таким образом, сдержать распространение вредоносных программ, сократить их уровень возможно лишь путем осуществления широкомасштабной научно обоснованной программы предупреждения, к разработке и реализации которой должны быть привлечены самые различные органы и организации, а также специалисты многих отраслей знаний.

---

[187] См.: Осипенко А.Л. Указ. соч. С. 420-421.

ЗАКЛЮЧЕНИЕ

Стремительное развитие компьютерных технологий и сетей, как неотъемлемой части современной телекоммуникационной системы, без использования возможностей которой уже невозможно представить деятельность абсолютного большинства институтов различных стран мира, является одним из основных факторов, способствующих росту компьютерной преступности, которая становится одним из наиболее опасных видов преступных посягательств. Основным средством борьбы с преступлениями в данной сфере, на наш взгляд, должно быть уголовное законодательство, которое на протяжении последних лет активно развивается как в зарубежных странах, так и в России.

Однако, необходимо отметить, что не существует единой терминологии для обозначения преступлений в сфере компьютерной информации. Это связано с отсутствием единой доктринальной позиции по отнесению конкретных противоправных деяний к таким преступлениям в связи с постоянными изменениями информационных компьютерных технологий.

По нашему мнению, преступления в сфере компьютерной информации – это противоправные виновно совершенные наказуемые в уголовном порядке общественно опасные деяния, посягающие на общественные отношения, обеспечивающие безопасное производство, хранение и использование компьютерных информационных ресурсов и их защиту и причинившие вред, либо создавшие угрозу причинения вреда охраняемым законом правам и интересам физических и юридических лиц, общества, государства. Предметом таких преступлений выступает компьютерная информация. Под компьютерной информацией как предметом преступного посягательства следует понимать совокупность фактических данных и команд, зафиксированных на машинном носителе или передающихся по телекоммуникационным каналам связи, предназначенных для использования в компьютере, компьютерной системе или сети, имеющим собственника, установившего правила пользования ими.

По нашему мнению, вредоносную компьютерную программу можно определить как специально созданную или модифицированную компьютерную программу, способную совершать действия, приводящие к несанкционированному собственником информационной системы уничтожению, блокированию, модификации либо копированию информации, хранящейся в компьютере, компьютерной системе, сети или на машинных носителях. Понятие «вредоносная программа» является родовым по отношению к понятию «компьютерный вирус». Смешение таких понятий как «вредоносная» и «вирусная» программа ведет к неоправданному сужению признаков объективной стороны рассматриваемого преступления, что создает возможность для безнаказанности за незаконный оборот вредоносных компьютерных программ, не являющихся по своим качественным характеристикам вирусными.

В целях совершенствования уголовного законодательства, регулирующего ответственность за незаконный оборот вредоносных компьютерных программ, предлагается внести ряд изменений в ст. 273 УК РФ. Прежде всего, в названии и диспозиции ст. 273 необходимо использовать единственное число по

отношению к предмету преступления, во избежание фактической декриминализации деяний, а также ошибок, допускаемых в процессе правоприменения.

В связи с тенденцией омолаживания компьютерной преступности, на наш взгляд, было бы целесообразно снизить возраст уголовной ответственности по ст. 273 УК РФ до 14 лет и внести в ст. 20 УК РФ соответствующие изменения.

Под компьютерной преступностью, на наш взгляд, следует понимать вид массового социально негативного общественно опасного поведения, запрещенного уголовным законом, складывающегося из противоправных посягательств на общественные отношения, обеспечивающие безопасное производство, хранение и использование компьютерных информационных ресурсов и их защиту, характеризующийся высоким уровнем латентности, международным и организованным характером, наличием признаков профессиональной преступности, постоянным совершенствованием способов совершения преступлений для обеспечения безопасности незаконной деятельности. Проведенный анализ компьютерной преступности и ее проявлений на современном этапе позволяет выявить ряд тенденций в ее развитии. Во-первых, это продолжение процесса значительного роста количества преступлений в сфере компьютерной информации, и как следствие, увеличение ущерба, причиняемого данными преступлениями. Во-вторых, констатируется перенос центра тяжести на совершение компьютерных преступлений с использованием компьютерных сетей, и прежде всего Интернет. В-третьих, увеличение доли корыстных компьютерных преступлений будет, как нам представляется, усиливаться, что представляет наибольшую опасность для финансовой и производственной сферы. Четвертая тенденция вызывает особую тревогу и обеспокоенность за будущее страны. Она связана с демографической характеристикой компьютерной преступности и обнаруживает себя в омоложении компьютерных преступников, которое синхронизирует с общим омоложением преступности.

Особенностью комплекса причин компьютерной преступности в целом, и преступности, связанной с незаконным оборотом вредоносных программ в частности заключается в формировании мотивации субъекта и решения совершить подобное преступление под влиянием изменений, связанных с переходом мирового сообщества на новые технологические средства производства и информационного обеспечения.

Ведущую роль в причинном комплексе преступности, связанной с незаконным оборотом вредоносных программ, играют деформации экономического, правового и нравственного сознания, на индивидуальном уровне реализуемые в корыстной мотивации, правовом нигилизме и убежденности в собственной безнаказанности. Формирующими эти причины условиями выступают: переход к информационному обществу, последствия неудачных экономических реформ, недостатки государственной политики в информационной сфере, недостатки уголовного законодательства, регулирующего отношения в сфере безопасности компьютерной информации, разрушение системы нравственных ценностей, негативное влияние сетевой среды, высокий уровень латентности компьютерных преступлений.

Условия, способствующие совершению преступлений, связанных с незаконным оборотом вредоносных программ, проявляются в низком уровне компьютерной культуры населения, а также в недостаточной квалификации работников правоохранительных органов, слабом техническом и материальном обеспечении подразделений, осуществляющих борьбу с компьютерной преступностью.

Анализ уголовных дел показывает, что подобные преступления в подавляющем большинстве совершаются лицами мужского пола, среди которых преобладают молодые люди в возрасте от 18 до 24 лет. Однако в последнее время существует тенденция к омоложению компьютерных преступников. Образовательный уровень таких преступников достаточно высок. Среди наиболее распространенных качеств таких преступников преобладают правовой нигилизм и завышенная самооценка.

Типологизация личности компьютерного преступника может проводиться по различным основаниям (например, по особенностям мотивации, по уровню подготовленности, преступной специализации и т. д.). Такие сведения позволяют наиболее полно составить обобщенный криминологический портрет субъекта, совершающего преступления, связанные с незаконным оборотом вредоносных программ.

При криминологической характеристике личности преступников, совершающих преступления, связанные с незаконным оборотом вредоносных программ, считаем, что их можно классифицировать в зависимости от характера совершаемых деяний и различиях в профессиональных навыках этих лиц на три группы: создателей, пользователей и распространителей.

Для эффективного предупреждения преступности, исследуемого вида, представляется целесообразным акцентировать внимание на трех основных группах специально-криминологических мер, составляющих в своей совокупности целостную систему борьбы с этим социально опасным явлением, а именно: правовых, технических и организационных.

Первая группа предполагает совершенствование правовых механизмов, которое должно осуществляться в трех направлениях: совершенствование отечественного уголовного законодательства, устанавливающего ответственность за подобные преступления; формирование правового фундамента в сфере Интернета; разработка и реализация стратегии международного сотрудничества в сфере противодействия преступности такого вида.

Вторая группа мер предусматривает совершенствование технических средств защиты, прежде всего физических (инженерные средства и сооружения, препятствующие физическому проникновению на объекты защиты), программно-аппаратных (приборы, устройства, и другие технические решения, а также специальные программы, программные комплексы и системы защиты информации) и криптографических (методы преобразования информации, основой которых является шифрование).

Третья группа предусматривает предотвращение преступлений за счет осуществления мероприятий организационного характера, таких как, налаживание сотрудничества между органами, осуществляющими борьбу с преступно-

стью в сфере компьютерной информации и субъектами информационного оборота; организация системы подготовки и переподготовки среди работников правоохранительных органов специалистов соответствующего профиля; создание центров анализа подобной преступности; распространение информации об успешной борьбе с такой преступностью, а также об опасности и противозаконности подобных деяний; введение образовательных программ, повышающих информационную культуру граждан; создание на предприятиях, которые являются пользователями глобальных сетей, специальных административных служб, в компетенцию которых входит организация всех мероприятий по информационной безопасности и защите информации.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Официальные документы и нормативно-правовые акты

1. Конституция РФ (принята всенародным голосованием 12.12.1993) // Российская газ. – 1993. – 25 дек.

2. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г. // Бюллетень международных договоров. – 2002. – № 11.

3. Кодекс РФ об административных правонарушениях от 30 декабря 2001 г. №196-ФЗ // Собрание законодательства РФ. – 2002. – №1 (1 ч.). – Ст. 1; 2007. – № 31. – Ст. 4009.

4. Гражданский кодекс РФ (часть вторая) от 26 января 1996 г. №14-ФЗ // Собрание законодательства РФ. – 1996. – № 5. – Ст. 410; 2007. – № 50. – Ст. 6247.

5. Гражданский кодекс РФ (часть четвертая) от 18 декабря 2006 г. №230-ФЗ // Собрание законодательства РФ. – 2006. – № 52 (1ч). – Ст. 5496; 2007. – № 49. – Ст. 6079.

6. Уголовный кодекс РФ от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954; 2007. – № 50. – Ст. 6248.

7. Уголовно-процессуальный кодекс РФ от 18 декабря 2001 г. №174-ФЗ // Собрание законодательства РФ. – 2001. – № 52 (1ч). – Ст. 4921; 2008. – №12. – Ст. 1074.

8. О государственной тайне: Закон РФ от 21 июля 1993 № 5485-1 // Российская газ. – 1993. – 21 сент; Собрание законодательства РФ. – 2007. – № 49. – Ст. 6079.

9. Об информации, информационных технологиях и о защите информации: Закон РФ от 27 июля 2006 г. № 149-ФЗ // Собрание законодательства РФ. – 2006. – № 31(1ч.). – Ст. 3448.

10. Об электронной цифровой подписи: Закон РФ от 10 января 2002 г. № 1-ФЗ // Собрание законодательства РФ. – 2002. – № 2. – Ст. 127; 2007. – № 46. – Ст. 5554.

11. О связи: Закон РФ от 7 июля 2003 г. №126-ФЗ // Собрание законодательства РФ. – 2003. – № 28. – Ст. 2895; 2007. – №1(1ч.). – Ст. 8.

12. Об утверждении Концепции национальной безопасности: Указ Президента РФ от 17 декабря 1997 г. №1300 // Российская газ. – 1997. – 26 дек.; Собрание законодательства РФ. – 2000. – № 2. – Ст. 170.

13. Об утверждении перечня сведений конфиденциального характера: Указ президента РФ от 6 марта 1997 г. №188 // Собрание законодательства. – 1997. – № 10. – Ст. 1127; Собрание законодательства. – 2005. – № 39. – Ст. 3925.

14. О концепции правовой информатизации: Указ Президента РФ от 28 июня 1993 г. № 966 // Собрание актов Президента РФ и Правительства РФ. – 1993. – № 27. – Ст. 2521; Собрание законодательства РФ. – 2005. – № 13. – Ст. 1137.

15. О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления шифровальных услуг в области шифрования информации: Указ Президента РФ от

3 апреля 1995 г. № 334 // Собрание законодательства РФ. – 1995. – № 15. – Ст. 1285; 2000. – № 31. – Ст. 3252.

16. Об основах государственной политики в сфере информатизации: Указ президента РФ от 20 января 1994 г. №170 // Собрание актов Президента РФ и Правительства РФ. – 1994. – № 4. – Ст. 305; Собрание законодательства РФ. – 1997. – № 28. – Ст. 3422.

17. О подписании Конвенции о киберпреступности: Распоряжение Президента РФ от 15 ноября 2005 г. № 557-рп // Собрание законодательства РФ. – 2005. – № 47. – Ст. 4929.

18. Доктрина информационной безопасности РФ (утверждена Президентом РФ 9 сентября 2000 г. № Пр-1895) // Российская газ. – 2000. – 28 сент.

19. О судебном приговоре: Постановление Пленума Верховного Суда РФ от 29 апреля 1996 г. №1 // Бюллетень Верховного Суда РФ. – 1996. – №1; 2007. – № 5.

Книги, монографии, учебные пособия

20. Агапов А.Б. Основы государственного управления в сфере информатизации в Российской Федерации. – М.: Юристъ, 1997. – 344 с.

21. Андреев Б.В. Правовая информатика: Учебное пособие . – М.: Институт международного права и экономики им. А.С. Грибоедова, 1998. – 128 с.

22. Андреев Б.В. Расследование преступлений в сфере компьютерной информации / Б.В. Андреев, П.Н. Пак, В.П. Хорст. – М.: Юрлитинформ, 2001. – 151 с.

23. Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ – Санкт-Петербург, 2000. – 152 с.

24. Антонян Ю.М. Психология преступника и расследования преступлений / Ю.М. Антонян, М.И. Еникеев, В.Е. Эминов. – М.: Юристъ, 1996. – 335 с.: ил.

25. Айков Д. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями: Перевод с английского / Д. Айков, К. Сейгер, У. Фонсторх. – М.: Мир, 1999. – 351 с.

26. Батурин Ю. М. Проблемы компьютерного права. – М.: Юридическая литература, 1991. – 271 с.

27. Батурин Ю.М. Компьютерная преступность и компьютерная безопасность / Ю. М. Батурин, А. М. Жодзишский. – М.: Юридическая литература, 1991. – 160 с.

28. Бачило И.Л. Информационное право: Учебник / И.Л. Бачило, В.Н. Лопатин, М.А. Федотов; под. ред. Б.Н. Топорнина. – СПб.: Изд-во «Юридический центр Пресс», 2001. – 789 с.

29. Безруков Н.Н. Классификация компьютерных вирусов MS DOS и методы защиты от них. – М.: СП «ICE», 1990 – 48 с.

30. Безруков Н.Н. Компьютерные вирусы. – М.: Наука,1991. – 158 с.

31. Беккариа Ч. О преступлениях и наказаниях. – М.: Инфа-М, 2004. – 184 с.

32. Белинская Е.П. Человек в информационном мире. – М.: АспектПресс, 2002. – 45 с.

33. Белкин П.Ю. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учебное пособие для вузов / П.Ю. Белкин, О.О. Михальский, А.С. Першаков и др. – М.: Радио и связь, 1992. – 168 с.

34. Василькова В.В. Порядок и хаос в развитии социальных систем: (Синергетика и теория социальной самоорганизации). – СПб.: Лань, 1999. – 480 с.

35. Венгеров А.Б. Право и информация в условиях автоматизации управления: (Теоретические вопросы). – М.: Юрид. лит., 1978. – 208 с.

36. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия. – М.: Право и Закон, 1996. – 182 с.

37. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: ООО Издательство «Юрлитинформ», 2002. – 496 с.

38. Воронина Т.П. Информационное общество: сущность, черты, проблемы. – М.: ЦАГИ, 1995. – 110 с.

39. Гаврилов М.В. Осмотр при рассмотрении преступлений в сфере компьютерной информации / М.В. Гаврилов, А.Н. Иванов. – М.: Юрлитинформ, 2007. – 152 с.

40. Горяинов К.К. Транснациональная преступность / К.К. Горяинов, А.П. Исиченко, Л.В. Кондратюк. – М.: ВНИИ МВД, 1997. – 260 с.

41. Грень И.В. Компьютерная преступность. – М.: Новое знание, 2007. – 416 с.

42. Гульев И.А. Создаем вирус и антивирус. – М.: ДМК, 1999. – 304 с.

43. Гуров А.И. Профессиональная преступность. – М.: Юрид. лит., 1990. – 301 с.

44. Згадзай О.Э. Преступления в сфере компьютерной информации: Аналитический обзор / О.Э. Згадзай, С.Я. Казанцев, Р.М. Оболенский. – Казань, 2003. – 123 с.

45. Зуев К.А. Компьютер и общество. – М.: Политиздат, 1990. – 314 с.

46. Информатика в терминах и определениях российского законодательства / Под ред. В.А. Никитова. – М: Славянский диалог, 2000. – 431 с.

47. Информатика и математика для юристов. Сеть Интернет: Учебное пособие / Под ред. проф. В.Д. Элькина. – М.: Профобразование, 2003. – 182 с.

48.Информационное общество: Информационные войны. Информационное управление. Информационная безопасность / Под ред. М.А. Вуса. – СПб.: Изд-во С.-Петербург. ун-та, 1999. – 212 с.

49. Карпец И.И. Преступность: Иллюзии и реальность. – М.: Рос. право, 1992. – 431 с.

50. Каспаров А.А. Создание использование и распространение вредоносных программ для ЭВМ: уголовно-правовые аспекты: Лекция. – М.: ТИССО, 2003. – 40 с.

51. Касперский Е.В. Компьютерные вирусы в MS DOS. – М.: ЭДЭЛЬ, 1992. – 176 с.

52. Касперский Е.В. Компьютерные вирусы: что это такое и как с ними бороться. – М.: СК Пресс, 1998. – 288 с.

53. Кастельс М. Информационная эпоха. Экономика, общество и культура. – М.: ГУ ВШЭ, 2000. – 608 с.

54. Коваль И. Как написать компьютерный вирус. Практика программирования на ассемблере. – СПб.: Символ-Плюс, 2000. – 192 с.

55. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. – М.: Горячая линия-Телеком, 2002. – 336 с.: ил.

56. Комментарий к Уголовному кодексу Российской Федерации. – Изд. 3-е, изм. и доп. / Под общей ред. Ю.И. Скуратова, В.М. Лебедева. – М.: Издательская группа НОРМА – ИНФА, 1999. – 896 с.

57. Комментарий к Уголовному Кодексу Российской Федерации / Под ред. А.В. Наумова. – М.: Юрист, 1996. – 824 с.

58. Комментарий к Уголовному Кодексу Российской Федерации / Отв. ред. В.И. Радченко. – М.: Вердикт, 1996. – 648 с.

59. Красавчиков О.А. Возмещение вреда, причиненного источником повышенной опасности. – М.: Юрид. лит., 1966. – С. 65-66.

60. Криминология / Под общ. ред. А.И. Долговой. – М: Норма, 2005. – 912 с.

61. Криминология / Под ред. Н.Ф. Кузнецовой, Г.М. Миньковского. – М.: Изд-во МГУ, 1998. – 414 с.: ил.

62. Криминология: Учебник для вузов / Под ред. проф. В.Д. Малкова. – 2-е изд. – М.: ЗАО «Юстицинформ», 2006. – 528 с.

63. Крылов В.В. Информационные компьютерные преступления. – М.: Издательская группа ИНФА-М-НОРМА, 1997. – 285 с.

64. Крылов В.В. Расследование преступлений в сфере информации. – М.: Издательство «Городец», 1998. – 264 с.

65. Кудрявцев В.Н. Генезис преступления: Опыт криминологического моделирования: Учебное пособие. – М.: Инфа-М, 1998. – 216 с.

66. Кудрявцев В.Н. Причины преступности в России: Криминологический анализ / В.Н. Кудрявцев, В.Е. Эминов. – М.: Норма, 2006. – 112 с.

67. Кузнецова Н.Ф. Преступление и преступность. – М.: Изд-во Моск. ун-та, 1969. – 250 с.

68. Кузнецова Н.Ф. Проблемы криминологической детерминации / Под ред. В.Н. Кудрявцева. – М: Изд-во Моск. ун-та, 1984. – 200 с.

69. Курс советской криминологии. В 2-х т. Т. 1 / Под ред. В. Н. Кудрявцева. – М.: Юрид. лит., 1985. – 415 с.

70. Курс уголовного права. В 5 т. Том 4. Особенная часть / Под ред. Г.Н. Борзенкова, В.С. Комиссарова. – М.: Зерцало-М, 2002. – 672 с.

71. Курушин В.Д. Компьютерные преступления и информационная безопасность / В.Д. Курушин, В.А. Минаев. – М.: Новый юрист, 1998. – 256 с.

72. Левин М. Как стать хакером: Справочник. – М.: Оверлей, 2001. – 326 с.

73. Левин М. Руководство для хакеров. – М.: Оверлей, 2001. – 416 с.

74. Левин М. Секреты компьютерных взломщиков: Крэкинг. – М.: Познавательная книга плюс, 2001. – 224 с.

75. Леонтьев Б. Хакеры & Internet. – М.: Познавательная книга, 1998. – 430 с.

76. Леонтьев Б. Хакеры, взломщики и другие информационные убийцы. – М.: Познавательная книга, 1999. – 192 с.

77. Ломов Б.Ф. Методологические и теоретические проблемы психологии. – М.: Наука, 1999. – 349 с.

78. Лунеев В.В. Преступность XX века: мировой криминологический анализ. – М.: Норма, 1997. – 480 с.

79. Лунев В.В. Мотивация преступного поведения. – М.: Наука, 1991. – 290 с.

80. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. – М.: Горячая линия-Телеком, 2004. – 280 с.: ил.

81. Мельников В.В. Защита информации в компьютерных системах. – М.: Финансы и статистика, 1997. – 368 с.

82. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография. – М.: Норма, 2004. – 432 с.

83. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448 с.

84. Правовая информатика и кибернетика / Под ред. Н.С. Полевого. – М.: Юрид. лит., 1993. – 527 с.

85. Преступления в сфере компьютерной информации: квалификация и доказывание: Учебное пособие / Под ред. Ю.В. Гаврилина. – М.: ЮИ МВД РФ, 2003. – 245 с.

86. Попов С. Сознание и социальная среда. – М.: Прогресс, 1979. – 231 с.

87. Русско-английский толковый словарь по информатике / В.И. Першиков, А.С. Марков, В.М. Савинков. – 3-е изд. – М.: Финансы и статистика, 1999. – 363 с.

88. Российское уголовное право. Особенная часть / Под ред. В.Н. Кудрявцева, А.В. Наумова. – М.: Юристъ, 1997. – 350 с.

89. Репецкая А.Л. Криминология: Общая часть: Учеб. пособие / А.Л. Репецкая, В.Я. Рыбальская. – Иркутск: ИГЭА, 1999. – 237 с.

90. Савельева И.В. Правовая охрана программного обеспечения ЭВМ // Право и информатика. – М.: МГУ, 1990. – С. 9-24.

91. Селиванов Н.А. Расследование особо опасных преступлений. Пособие для следователей. – М.: Бек, 1998. – 165 с.

92. Симкин Л.С. Программы для ЭВМ: правовая охрана (правовые средства против компьютерного пиратства). – М.: Издательство «Городец», 1998. – 208 с.

93. Скоромников К.С. Компьютерное право Российской Федерации: Учебник. – М.: Изд-во МНЭПУ, 2000. – 224 с.

94. Соловьев Л.Н. Вредоносные программы: расследование и предупреждение преступлений. – М.: Собрание, 2004. – 224 с.

95. Старостина Е.В. Защита от компьютерных преступлений и кибертерроризма / Е.В. Старостина, Д.Б. Фролов. – М.: Изд-во Эксмо, 2005. – 192 с.

96. Степанов Е.А. Управление персоналом: Персонал в системе защиты информации: Учебное пособие. – М.: Форум, 2002. – 288 с.

97. Уголовное право. Особенная часть / Отв. ред. И.Я. Козаченко – М.: ИНФРА-М-НОРМА, 1997. – 768 с.

98. Уголовное право. Особенная часть: Учебник / Под ред. А.И. Рарога. – М.: Триада, Лтд, 1996. – 480 с.

99. Уголовное право РФ. Особенная часть: Учебник / Отв ред. Б.В. Здравомыслов. – М.: Юрист, 1996. – 560 с.

100. Уголовное право. Особенная часть / Под ред. Г.Н. Борзенкова и В.С. Комиссарова. – М.: Олимп, 1997. – 752 с.

101. Фролов А.В. Осторожно: компьютерные вирусы / А.В. Фролов, Г.В. Фролов. – М.: ДИАЛОГ-МИФИ, 1996. – 256 с.

102. Файтс Ф. Компьютерный вирус: проблемы и прогноз: Пер. с англ. / Ф. Файтс, П. Джонстон, М. Кратц. – М.: Мир,1994. – 176 с.

103. Фэри Д. Секреты супер-хакера. – СПб: Невский проспект, 1997. – 384 с.

104. Хокинс Дж.М. The Oxford dictionary of the English Language (Оксфордский толковый словарь английского языка). – Oxford University Press, Астрель, АСТ, 2001. – 832 с.

105. Черкасов В.Н. Борьба с экономической преступностью в условиях применения компьютерных технологий: Учеб. пособие. – Саратов: СВШ МВД РФ, 1995. – 87 с.

106. Черкасов В.Н. Теория и практика решения организационно-методических проблем борьбы с экономической преступностью в условиях применения компьютерных технологий. – М.: Юрист, 1994. – 135 с.

107. Шинкаренко И.Р. Преступления в сфере исполнения компьютерной техники: квалификация, расследование и противодействие: Монография / И.Р. Шинкаренко, В.О. Голубев, Н.В. Карчевський. – Донецк: РВВ ЛДУВС, 2007. – 267 с.

108. Ярочкин В.И. Безопасность информационных систем. – М.: «Ось-89», 1996. – 320 с.

Статьи

109. Агарков М.М. Обязательства из причинения вреда // Проблемы социалистического права. – 1936. – № 1. – С. 51-60.

110. Антонян Ю.М. Концепция причин преступности и причины преступности в России // Российский следователь. – 2004. – № 8. – С. 26-32.

111. Андриенко Ю.В. В поисках объяснения роста преступности в России в переходный период: криминометрический подход // Экономический журнал ВШЭ. – 2001. – № 2. – С. 194-220.

112. Борчева Н.А. Компьютерное право и ответственность за компьютерные преступления за рубежом // На пути к информационному обществу: криминальный аспект. Сборник статей. – М., 2002. – С. 15-18.

113. Быков В. Совершенствование уголовной ответственности за преступления, сопряженные с компьютерными технологиями / В. Быков, А. Нехорошев, В. Черкасов // Уголовное право. – 2003. – № 3. – С. 9-11.

114. Вехов В.Б. Аспекты борьбы с преступлениями, совершенными с использованием сети Интернет // Интеллектуальная ответственность. – 2004. – № 11. – С. 46-52.

115. Вехов В.Б. Правовые и криминалистические аспекты понятия компьютерной информации // «Черные дыры» в Российском законодательстве. – 2004. – № 3. – С. 234 – 248.

116. Волеводз А.Г. Российское законодательство об уголовной ответственности за преступления в сфере компьютерной информации // Российский судья. – 2002. – № 9. – С. 34-41.

117. Вихорев С. Практические рекомендации по информационной безопасности / С. Вихорев, А. Ефимов // JetInfo. – 1996. – № 7. – Т. 2. – С. 42-48.

118. Голосков Л.В. Сетевое законодательство: концепция развития // Информационное право. – 2006. – № 4 (7). – С. 11-14.

119. Голубев В. Электронный терроризм – новое лицо терроризма // 2-я Мировое сообщество против глобализации преступности и терроризма: Международная конференция. – М.: Изд. «Экономика», 2004. – С. 146-150.

120. Грибанов Д.В. Кибернетический терроризм: новая угроза общественной безопасности // Российский юридический журнал. – 2004. – №4. – С. 75-79.

121. Гульбин Ю. Преступления в сфере компьютерной информации // Российская юстиция. – 1997. – № 10. – С. 24-25.

122. Дамаскин О.В. Актуальные вопросы законодательного обеспечения национальной безопасности в условиях глобализации // Системы безопасности. – 2003. – № 3. – С. 90-91.

123. Долгишев В. Обвинение с компьютерным уклоном. Практика уголовного дела // Адвокатские вести. – 2002. – № 2. – С. 16-18.

124. Долгова А.И. Взаимодействие и причинность в криминологии // Вопросы борьбы с преступностью. – М., 1981. Вып. 34. – С. 23-30.

125. Домозетов Х. Социологические проблемы компьютерного пиратства // Социологические исследования. – 1997. – № 11. – С. 110-114.

126. Завидов Б.Д. О правовом значении подписи и электронной цифровой подписи на документах / Б.Д. Завидов, В.Б. Липатенков // Право и экономика. – 2001. – № 1. – С. 8-14.

127. Закупень Т.В. Информационно-поисковые системы для органов государственной власти // Проблемы информатизации. – 1997. – № 3. – С. 53-57.

128. Зубков А. Кевин Митник вышел на свободу // Мир Internet. – 2000. – № 3. – С. 48-49.

129. Компьютерная преступность: уголовно-правовые и криминологические проблемы (Международная научно-практическая конференция) // Государство и право. – № 9. – С. 101-106.

130. Корни-Мюррей Э. Сколько стоит компьютерное преступление: Защита информации от хакеров // LAN: Журнал сетевых решений. – 2002. – № 5. – С. 82-87.

131. Кочои С. Ответственность за неправомерный доступ к компьютерной информации / С. Кочои, Д. Савельев // Российская юстиция. – 1999. – № 1. – С. 23-26.

132. Кребер Г. Категория условия и соотношение ее с категорией причины // Философские науки. – 1961. – № 3. – С. 115-121.

133. Кристальный Б. Концепция российского законодательства в области Интернета / Б. Кристальный, М. Якушев // Информационные ресурсы России. – 2000. – № 2. – С. 19-25.

134. Крутских А.В. Информационный вызов безопасности на рубеже XXI века // Международная жизнь. – 1999. – № 2. – С. 82-89.

135. Кузнецов А. Пираты в Интернете // Милиция. – 2000. – № 2. – С. 27-29.

136. Кутафин О.Е. Проблемы становления информационного права в России / О.Е. Кутафин, В.А. Копылов // Сборник НТИ. – Серия 1. – 1999. – № 8. – С. 19-20.

137. Линде С. Несанкционированный доступ – примеры вторжения // Открытые системы. – 1996. – № 4 (18). – С. 28-30.

138. Ляпунов Ю. Ответственность за компьютерные преступления / Ю. Ляпунов, В. Максимов // Законность. – 1997. – № 1. – С. 8-15.

139. Макаров Н.И. Актуальные проблемы правопонимания в информационном обществе // Информационное право. – 2007. – № 1. – С. 4-6.

140. Мещереков В.А. Криминалистическая классификация преступлений в сфере компьютерной информации // Защита информации: Конфидент. – 1999. – № 4-5 (27). – С. 17-19.

141. Морозов А.В. Некоторые аспекты информатизации системы юстиции // НТИ. – Сер.1. – 1999. – № 9. – С. 14-21.

142. Мотуз О.В. Виртуальный терроризм – реальность нашего времени // Защита информации: Конфидент. – 1999. – № 1-2 (25). – С. 69-74.

143. Никифоров И.В. Уголовно-правовые меры борьбы с компьютерной преступностью и обеспечение компьютерной безопасности // Вестник Санкт-Петербургского Университета. – Сер. 6. – 1995. – Вып. № 4 (27). – С. 90-96.

144. Номоконов В.А. Новые информационные технологии в борьбе с преступностью // Российский криминологический взгляд. – 2005. – № 1. – С. 90-93.

145. Овчинский А.С. Анализ опыта использования современных информационных технологий преступными группировками; хакерские технологии в сети Интернет / А.С. Овчинский, И.А. Наумов // Консультационно-информационный семинар «Хакеры против банков». – М., 1998. – С. 12-13.

146. Пархомов В.А. К определению понятия «Информационное преступление» // Вестник ИГЭА. – 2001. – № 2. – С.10-13.

147. Подольный Н.А. Некоторые особенности выявления, раскрытия и расследования компьютерных преступлений / Н. Подольный, А. Ширманова // Российский следователь. – 2004. – № 1. – С. 9-14.

148. Семенов Н.В. Экспертные исследования по делам о преступлениях, совершаемых в сфере высоких технологий // Бюллетень Министерства юстиции РФ. – 2001. – № 1. – С. 120-121.

149. Семилетов С. И. Информация как особый нематериальный объект права // Государство и право. – 2000. – № 5. – С. 67-74.

150. Середа С.А. Расширительное толкование терминов «вредоносная программа» и «неправомерный доступ» / С.А. Середа, Н.Н. Федотов // Закон. – 2007. – № 6. – С. 191-203.

151. Собчак А.А. О понятии источника повышенной опасности в гражданском праве // Правоведение. – 1964. – № 2. – С. 144-147.

152. Степанов-Егиянц В. Ответственность за компьютерные преступления // Законность. – 2005. – № 12. – С. 49-51.

153. Степанов-Егиянц В. К вопросу о терминологии в сфере компьютерных преступлений // «Черные дыры» в российском законодательстве. – 2005. – №4. – С. 218-221.

154. Стрельцов А.А. Направления совершенствования правового обеспечения информационной безопасности Российской Федерации // Информационное общество. – 1999. – № 6. – С. 15-20.

155. Султанаева Г.Я. Опыт криминализации киберпреступлений в уголовном законодательстве // Соискатель. – 2004. – № 1. – С. 102-105.

156. Сырков Б. Троянские программы // Системы безопасности, связи и телекоммуникации. – 1999. – № 30. – С. 66-69.

157. Тедеев А.А. Особенности правового регулирования отношений в глобальных компьютерных сетях // Информационное право. – 2007. – № 2. – С. 7-9.

158. Широков В.А. Киберпреступность: история уголовно-правового противодействия / В.А. Широков, Е.В. Беспалова // Информационное право. – 2006. – № 4 (7). – С. 3-5.

159. Янг К.С. Диагноз – Интернет-зависимость // Мир Internet. – 2000. – № 2. – С. 24-29.

160. Ястребов Д.А. Институт уголовной ответственности в сфере компьютерной информации (опыт международно-правового сравнительного анализа) // Государство и право. – 2005. – №1. – С. 53-63.

161. Ястребов Д.А. Неправомерный доступ к компьютерной информации: вопросы последствий // Проблемы управления безопасностью сложных систем. Труды XIV Международной конференции. В 2-х т. Т. 1. – М.: ИЦ РГГУ, 2006. – С. 74-79.

162. IBM Global Security Analysis // Computer World Россия. – 1999. – № 11. – С. 29-30.

Диссертации и авторефераты диссертаций

163. Акутаев Р.М. Криминологический анализ латентной преступности: Автореф. … дис. д-ра юрид. наук. – СПб., 1999. – 42 с.

164. Бессонов В. А. Виктимологические аспекты предупреждения преступлений в сфере компьютерной информации: Дис. ... канд. юрид. наук. – Н. Новгород, 2000. – 249 с.

165. Бражник С. Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: Дис. … канд. юрид. наук. – Ижевск, 2002. – 189 с.

166. Бытко С. Ю. Некоторые проблемы уголовной ответственности за преступления, совершаемые с использованием компьютерных технологий: Дис. ... канд. юрид. наук. – Саратов, 2002. – 204 с.

167. Вехов В.Б. Криминалистическая характеристика и совершенствование практики расследования и предупреждения преступлений, совершаемых с использованием средств компьютерной техники: Дис. ... канд. юрид. наук. – Волгоград, 1995. – 282 с.

168. Воробьев В.В. Преступления в сфере компьютерной информации: Юридическая характеристика составов и квалификация: Дис. ... канд. юрид. наук. – Н. Новгород, 2000. – 201 с.

169. Гаджиев М.С. Криминологический анализ преступности в сфере компьютерной информации: Дис. … канд. юрид. наук. – Махачкала, 2004. – 168 с.

170. Добровольский Д.В. Актуальные проблемы борьбы с компьютерной преступностью: уголовно-правовые и криминологические аспекты: Дис. … канд. юрид. наук. – М., 2005. – 218 с.

171. Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение: Дис. … канд. юрид. наук. – М., 2003. – 178 с.

172. Зинина У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: Автореф. дис. … канд. юрид. наук. – М., 2007. – 33 с.

173. Карпов В.С. Уголовная ответственность за преступления в сфере компьютерной информации: Дис. … канд. юрид. наук. – Красноярск, 2002. – 202 с.: ил.

174. Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: Дис. …д-ра юрид. наук. – М., 2006. – 418 с.

175. Малыковцев М.М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ: Дис. … канд. юрид. наук. – М., 2006. – 186 с.

176. Межега М.М. Криминалистические проблемы расследования создания, использования и распространения вредоносных программ для ЭВМ: Дис. … канд. юрид. наук. – Саратов, 2005. – 238 с.

178. Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: Дис. … канд. юрид. наук. – М., 1998. – 161 с.

179. Спирина С.Г. Криминологические и уголовно-правовые проблемы преступлений в сфере компьютерной информации: Дис. ... канд. юрид. наук. – Краснодар, 2000. – 216 с.

180. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: Автореф. дис. … канд. юрид. наук. – Владивосток, 2005. – 26 с.

181. Усов А.И. Концептуальные основы судебной компьютерно-технической экспертизы: Дис. ... д-ра юрид. наук. – М., 2002. – 372 с.

182. Ушаков С.И. Преступления в сфере обращения компьютерной информации: теория, законодательство, практика: Дис. ... канд. юрид. наук. – Ростов-на-Дону, 2000. – 176 с.

183. Шийко А.С. Политика борьбы с компьютерной преступностью как угрозой информационной безопасности России: Автореф. дис. … канд. юрид. наук. – М., 2001. – 30 с.

Литература на иностранном языке

184. Collin B. C. The Future of CyberTerrorism [Электронный ресурс] // Proceedings of 11th Annual International Symposium on Criminal Justice Issues. – The University of Illinois. Chicago, 1996. – Режим доступа: http://www.acsp.uic.edu/OICJ/CONFS/terror02.htm.

185. Hammond A. The 2001 Council of Europe Convention on cyber-crime: an efficient tool to fight crime in cyber-space? – Santa Clara University. Cedric J. Magnin. June, 2001. – 156 p.

186. Pollitt Mark M. A Cyberterrorism Fact or Fancy? // Proceedings of the 20th National Information Systems Security Conference, 1997. – P. 285-289.

187. Rogers M. A New Hacker Taxonomy. – Winniper, 2000. – 85 p.

188. Stallings W. Network and Internetwork Security Principles and Practice. – Englewood Cliffs, N. J.: Prentice Hall, 1995. – 130 p.

Монография

кандидат юридических наук
Маслакова Елена Александровна

НЕЗАКОННЫЙ ОБОРОТ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ: УГОЛОВНО-ПРАВОВЫЕ И КРИМИНОЛОГИЧЕСКИЕ ПРОБЛЕМЫ

Свидетельство о государственной аккредитации
Рег. № 1300 от 23.12.11 г.
Подписано в печать_____г. Формат 60x90$^{1}/_{16}$.
Усл. печ. л. 6,7. Тираж ____экз. Заказ № _____.

Орловский юридический институт МВД РФ.
302027, Орел, Игнатова, 2.