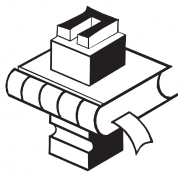
В. А. Мазуров

Компьютерные преступления

классификация и способы противодействия

Учебно-практическое пособие



Издательство «Палеотип»
Москва, 2002

УДК 343
ББК 67.408
М13

Рецензенты:

Р. М. Абызов, доктор юридических наук, полковник;
Д. П. Потапов, кандидат юридических наук, майор;
А. Г. Опалев, полковник.

Автор — кандидат юридических наук В. А. Мазуров.

М13 **Мазуров В. А. Компьютерные преступления: классификация и способы противодействия**: Учебно-практическое пособие. — М.: Издательство «Палеотип», 2002. — 148 с.

ISBN 5-94727-017-X

В настоящем учебном пособии рассматриваются понятие и уголовно-правовая характеристика состава преступления, предусмотренного ст. 272 УК РФ, проанализированы российское и зарубежное законодательство, научно-правовая литература, практика уголовно-правовой защиты информации в России.

Предназначено для студентов и преподавателей юридических вузов, а также практических работников правоохранительных органов.

ISBN 5-94727-017-X

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Одна из черт современного общества — бурное развитие научно-технического прогресса вообще и электронно-вычислительной техники в частности. Развитие информационной сферы, обеспечение ее безопасности становятся одними из приоритетных задач национальной политики промышленно развитых стран мира. Как считают специалисты, по темпам развития, влиянию на социально-экономическую инфраструктуру, вкладу в научно-техническую революцию, позитивным изменениям в интеллектуализации общества микроэлектронная и компьютерная отрасли промышленности, составляющие базу развития информационного пространства любой страны, не имеют аналогов. К 2000 г. они могут стать самыми мощными и наукоемкими в мире.

Однако расширение использования электронно-вычислительной техники породило не только технические, но и правовые проблемы. Серьезным негативным последствием компьютеризации общества являются так называемые "компьютерные преступления". Данная проблема, будучи новой для правоохранительных органов России, не имеет в настоящее время адекватного решения и по мере информатизации всех сторон деятельности общества становится все более острой. Именно это обусловливает актуальность и новизну предлагаемого исследования.

Термин "компьютерное преступление" стал впервые употребляться в американской, а затем и другой зарубежной литературе уже в начале 60-х гг., когда стали выявляться преступления, совершаемые с использованием ЭВМ. Позже этот термин стал широко использоваться в практической деятельности правоохранительных органов, хотя первоначально не имел под собой ни терминологического, ни правового обоснования. В на-

стоящее время термин "компьютерное преступление" признан большинством западных криминалистов.

В российской научной и особенно в публицистической литературе употребляются самые различные понятия, касающиеся подобного рода посягательств: компьютерные преступления, коммуникационные преступления, "кибербандитизм", информационные преступления, программные злоупотребления и т. д. Различие в терминологии указывает на отсутствие единого подхода к данной проблеме.

Вопрос о состоятельности этого понятия обсуждался и российскими юристами на очередном заседании постоянно действующего межведомственного семинара на тему: "Криминалистика и компьютерная преступность", организованного координационным бюро по криминалистике при НИИ проблем укрепления законности и правопорядка Генеральной прокуратуры и экспортно-криминалистическим центром МВД РФ в марте 1993 г. При этом в подходе к рассмотрению данной проблемы сложилось две точки зрения.

Одни авторы выступили против употребления данного термина, аргументируя свои возражения тем, что преступления не принято дифференцировать по виду технических средств, с помощью которых они совершаются[1].

Другие ученые (Ляпунов Ю., Максимов В., Скормников К., Селиванов Н., Вехов В., Никифорров И. и др.) признают состоятельность формулировки "компьютерное преступление", так как данный термин уже воспринят как зарубежной, так и отечественной практикой[1].

---

[1] *Батурин Ю. М.* "Компьютерное преступление" — что за термином? // Право и информатика / Под ред. *А. П. Суханова.* М.: Изд-во МГУ, 1990. С. 99; *Батурин Ю. М.* Проблемы компьютерного права. М.: Юридическая литература, 1991. С. 167; *Курило А. П.* О проблеме компьютерной безопасности // Научно-техническая информация. Сер. 1. Орг. и методика информ. работы. 1993. № 8. С. 7.

[2] *Селиванов Н.* Проблемы борьбы с компьютерной преступностью // Законность. 1993. № 8. С. 36—37; *Вехов В. В.* Компьютерные преступления: способы совершения и раскрытия / Под общ. ред. акад. *В. П. Смагоринского.* М.: Право и Закон, 1996. С. 20; *Никифоров И. В.* Уголовно-правовые меры борьбы с компьютерной преступностью и обеспечение компьютерной безопасности // Вестник Санкт-Петербургского университета. Сер. 6. Вып. 4. 1995. № 27. С. 94; *Ляпунов Ю., Максимов В.* Ответственность за компьютерные преступления // Законность. 1997. № 1. С. 9; Пособие для следователя. Расследование преступлений повышенной общественной опасности / Под ред. *Н. А. Селиванова* и *А. И. Дворкина.* М.: ООО "Лига Разум", 1998. С. 336.

В УК РФ, вступившем в действие с 1 января 1997 г., введены новые виды преступлений — "преступления в сфере компьютерной информации", выделенные в отдельную главу. Однако сам термин "компьютерное преступление" в УК РФ отсутствует. В связи с этим в литературе предлагается различать понятие "компьютерного преступления" в уголовно-правовом и криминолого-криминалистическом аспектах[1].

Проблемы правовой защиты компьютерной информации привлекли к себе внимание юристов ведущих зарубежных стран в 70—80-е гг., когда начался расцвет компьютерной техники. Появление и распространение в 70-х гг. компактных и сравнительно недорогих персональных компьютеров, по мере совершенствования которых стали размываться границы между мини- и большими ЭВМ, создало возможность подключения к мощным информационным потокам неограниченного круга лиц, привело к компьютеризации хозяйственной и управленческой деятельности, использованию компьютерной техники в космических исследованиях, обороне, атомной энергетике и других областях жизни общества, где нарушение работы такой техники чревато авариями и даже катастрофами с человеческими жертвами и огромным экономическим ущербом. Кроме того, появление компьютерных банков с информацией персонального характера делает неправомерный доступ к ней весьма опасным для прав и свобод человека.

В связи с этим встал вопрос о контролируемости доступа к информации, ее сохранности и доброкачественности. Организационные меры, а также программные и технические средства защиты оказались недостаточно эффективными. Особенно остро данная проблема дала о себе знать в странах с высокоразвитыми технологиями и информационными сетями. Вынужденные прибегать к дополнительным мерам безопасности, они активно стали использовать правовые средства защиты. Но традиционные меры гражданско-правовой и административной ответственности не смогли сыграть роль сдерживающего фактора и воспрепятствовать широкому распространению этого вида право-

[1] *Курило А. П.* Указ. соч. С. 7; *Батурин Ю. М.* "Компьютерное преступление" — что за термином? С. 97; *Вехов В. В.* Указ. соч. С. 23—25; Пособие для следователя. Расследование преступлений повышенной общественной опасности / Под ред. *Н. А. Селиванова* и *А. И. Дворкина.* С. 335.

нарушений. В связи с этим большое внимание в зарубежных странах стало уделяться развитию уголовного законодательства.

Под уголовно-правовыми мерами борьбы с компьютерной преступностью в литературе понимают принятие уголовно-правовых норм, устанавливающих уголовную ответственность за совершение отдельных деяний в сфере использования компьютерной техники[1]. Компьютерные преступления впервые попали в сферу специального контроля в начале 70-х гг. в США, когда было выявлено большое количество подобных деяний, совершенных в 50—70-е годы. Первым преступником, применившим ЭВМ для совершения налогового преступления на сумму 620 тыс. долл. и в 1969 г. представшим за это перед американским судом, стал Альфонсе Конфессоре, которого признали виновным 20 окружных судов США[2].

Этот факт привлек к сфере компьютерной информации пристальное внимание органов уголовной юстиции и ученых-криминологов. Начались интенсивные исследования этого феномена на национальном и международном уровнях, стали формулироваться специализированные нормы о компьютерных преступлениях в уголовных законодательствах.

Первоначально, столкнувшись с компьютерной преступностью, органы уголовной юстиции начали с ней борьбу при помощи традиционных правовых норм о краже, присвоении, мошенничестве и т. д. Однако такой подход оказался не вполне удачным, поскольку многие компьютерные преступления не охватываются составами традиционных преступлений.

Несоответствие криминологической реальности и уголовно-правовых норм потребовали развития последних. **Развитие это происходит в двух направлениях:**

1) более широкое толкование традиционных норм и их применение по аналогии;

2) разработка специализированных норм о компьютерных преступлениях.

Первое направление имеет свои естественные границы — предельная допустимость размывания признаков традиционных

---

[1] *Курушин В. Д., Минаев В. А.* Компьютерные преступления и информационная безопасность. М.: Новый юрист, 1998. С. 122.
[2] *Ляпунов Ю., Максимов В.* Указ. соч. С. 8.

составов (например, в 1979 г. в судебной практике во Франции по делу о лице, неправомерно сфотографировавшем чужие бумаги, было вынесено решение, допускавшее кражи информации; в 1983 г. информация была признана вещью в Нидерландах). Большинство европейских стран встало на второй путь — путь разработки специализированных норм о компьютерных преступлениях.

В 1973 г. в Швеции принимается закон, в соответствии с которым установлена ответственность за неправомерное изменение, уничтожение или доступ в отношении записей на компьютерных носителях (информационные злоупотребления). Впоследствии **специальные нормы о компьютерных преступлениях были приняты в США, Великобритании, Австрии, Канаде (июль 1985 г.), Дании (декабрь 1985 г.), Австралии, Франции, Португалии (1982 г.) и других странах.**

Уже в 70-х гг. в **США** все более настойчиво стали раздаваться требования подготовить и издать на федеральном уровне самостоятельные законодательные акты об ответственности за компьютерные преступления, максимально учитывающие их специфику. В связи с этим в 1977 г. в Сенат США был представлен проект "Закона о защите федеральных компьютерных систем". Однако соответствующий акт был принят Конгрессом США только в 1984 г., до этого практика шла по пути применения традиционных уголовно-правовых норм. Вскоре этот акт был дополнен новыми видами компьютерных преступлений и в настоящий момент называется "Закон 1986 года о мошенничестве и злоупотреблениях, связанных с компьютерами".

Необходимость издания законов, специально ориентированных на борьбу с компьютерными преступлениями, достаточно быстро была осознана в США на уровне законодательных органов отдельных штатов. К началу 70-х гг. соответствующие законы были изданы в шести штатах, а работа над законопроектами велась в двенадцати других. К 1985 г. такие акты были приняты в 47 штатах. Например, **в штате Флорида "Закон о компьютерных преступлениях"** вступил в силу с 1 января 1978 г. и является наиболее обстоятельным из всех аналогичных актов других штатов США. В соответствии с данным законом конкретные виды компьютерных преступлений разделены на три группы:

- преступления против интеллектуальной собственности, т. е. умышленное незаконное внесение изменений, уничтожение или похищение данных, программ и документации, связанной с компьютерами (ст. 815. 04);
- преступления, причиняющие вред компьютерному оборудованию, т. е. уничтожение или повреждение компьютерных систем, приборов и т. д. (ст. 815. 05);
- преступления, против пользователей компьютерами, т. е. любое незаконное использование чужого компьютера, в том числе попытка обработать на нем какие-либо данные, недопущение к пользованию компьютером лица, имеющего на это право (ст. 815. 06).

Серьезная реформа уголовного законодательства была предпринята в **Германии,** где в середине 70-х гг. разразилась дискуссия о целесообразности разработки уголовного законодательства применительно к преступным действиям в сфере использования ЭВМ. Прения и дебаты завершились принятием Бундестагом второго закона о борьбе с экономической преступностью, которым в УК ФРГ было введено семь новых параграфов, содержащих описание компьютерных преступлений. Например, Параграф 202а предусматривает уголовную ответственность лиц, неправомерно приобретающих для себя или иного лица непосредственно не воспринимаемые, записанные в устройстве памяти либо переданные данные, специально защищенные от несанкционированного доступа; Параграф 263а — уголовная ответственность для лица, оказавшего влияние на результаты обработки информации путем неправильного оформления программ (манипуляции с программным обеспечением), использования неправильных или неполных данных, а также посредством незаконного использования данных или воздействия на процесс обработки информации с помощью технических средств; Параграф 3036 — уголовная ответственность за компьютерный саботаж, т. е. самовольное нарушение процесса обработки данных посредством выведения из строя, изменения либо разрушения аппаратуры ЭВМ или носителя информации; Параграф 274 — уголовная ответственность за неправомочное стирание, уничтожение или частичное изменение важных данных, записанных в памяти компьютера, и др.[1]

[1] *Черных А.* Компьютерные преступления по УК ФРГ // Социалистическая законность. 1988. № 8. С. 66.

УК Франции (1992 г.) пополнил систему преступлений против собственности специальной главой "О посягательствах на системы автоматизированной обработки данных", где предусмотрел ответственность за незаконный доступ ко всей или части системы автоматизированной обработки данных, воспрепятствование работе или нарушение правильности работы такой системы или ввод в нее обманным способом информации, уничтожение или изменение базы данных. Не остались в стороне от этой проблемы и международные организации, в частности Совет Европы, который счел необходимым изучить и разработать проект специальной конвенции, посвященной проблеме правонарушений в сфере компьютерной информации[1].

Разработка соответствующей правовой базы в нашей стране началась в начале 90-х гг. Первоначально эта работа сводилась к изучению зарубежного опыта правового регулирования рассматриваемой области отношений. Прежде всего был проведен глубокий анализ уголовных законов США, Великобритании, Канады, Германии и Швейцарии, установивших ответственность как за совершение отдельных видов компьютерных преступлений (что наиболее характерно для англосаксонских стран), так и по их группам, относящим отдельные действия или бездействие с использованием компьютерной техники или в отношении нее к категории уголовных преступлений.

Определенным этапом на пути законодательного решения данной проблемы стало принятие в 1992 г. Закона РФ "О правовой охране программ для ЭВМ и баз данных"[2].

Закон содержал положения о том, что выпуск под своим именем чужой программы для ЭВМ или базы данных либо незаконное воспроизведение или распространение таких произведений влечет уголовную ответственность. Однако соответствующих изменений в УК РСФСР внесено не было.

Первой попыткой стал представленный проект закона РСФСР "Об ответственности за правонарушения при работе с информацией" (версия от 6 декабря 1991 г.).

---

[1] Уголовное право. Особенная часть: Учебник для вузов / Отв. ред. *И. Я. Козаченко, З. А. Незнамова, Г. П. Новоселов.* М.: ИНФРА-М—НОРМА, 1997. С. 55.

[2] Закон РФ "О правовой охране программ для ЭВМ и баз данных" // Ведомости съезда народных депутатов РФ и Верховного Совета РФ. 1992. № 42. Ст. 2325.

Проект содержал две части: в Общей части излагались основания и поводы наступления различных видов ответственности (дисциплинарной, гражданской, административной и уголовной) при совершении информационных и компьютерных правонарушений; в Особенной части описывались составы отдельных видов информационных и компьютерных правонарушений. Однако данный проект не дошел до окончательного рассмотрения в связи с тем, что многие из предлагаемых составов нуждались в доработке, особенно в уточнении объективных и субъективных сторон. В то же время, несмотря на многочисленные недоработки, данный проект имел важное практическое значение, так как определил дальнейшее направление этой работы.

В 1994 г. были разработаны еще два проекта внесения дополнительных составов преступлений по данной проблеме в УК РФ.

Первый вариант проекта предусматривал внесение изменений и дополнений в Кодекс РФ об административных правонарушениях, Уголовный и Гражданский кодексы в части установления ответственности за правонарушения при работе с информацией. В частности, в данном проекте предлагалось внесение в действующий УК следующих составов компьютерных преступлений:

- незаконное овладение программами для ЭВМ, файлами и базами данных (ст. 152-3);
- фальсификация или уничтожение информации в автоматизированной системе (ст. 152-4);
- незаконное проникновение в АИС, совершенное путем незаконного завладения парольно-ключевой информацией, нарушения порядка доступа или обхода механизмов программной защиты информации с целью ее несанкционированного копирования, изменения или уничтожения (ст. 152-5);
- внесение или распространение “компьютерного вируса” (ст. 152-6);
- нарушение правил, обеспечивающих безопасность АИС (ст. 152-7).

Кроме того, в данном проекте предлагалось введение самостоятельного состава преступления, совершаемого с использованием компьютерной техники в виде промышленного шпионажа (ст. 155-8).

Второй вариант проекта был разработан авторским коллективом, созданным государственно-правовым управлением при Президенте РФ в рамках нового законодательства. В рамках десятого раздела проекта была выделена глава 28 "Компьютерные преступления", в состав которой входили пять отдельных составов преступлений:

- **ст. 271. Самостоятельное проникновение в автоматизированную компьютерную систему (АКС);**
- **ст. 272. Неправомерное завладение программами для ЭВМ, файлами или базами данных;**
- **ст. 273. Самовольная модификация, повреждение, уничтожение баз данных или программ для ЭВМ;**
- **ст. 274. Внесение или распространение вирусных программ для ЭВМ;**
- **ст. 275. Нарушение правил, обеспечивающих безопасность информационных систем.**

Исходя из анализа предлагавшихся проектов, в литературе делается вывод о наличии единого подхода — введения самостоятельных составов собственно компьютерных преступлений. Создание дополнительных составов, как это предлагалось рядом авторов и используется в некоторых зарубежных странах, по признаку использования компьютерной техники, авторами проектов было признано нецелесообразным[1].

В проекте Уголовного кодекса, внесенного депутатами Государственной Думы — членами Комитета по законодательству и судебно-правовой реформе и Комитета по безопасности, указанные преступления были также объединены в главу 28 "Преступления в сфере компьютерной информации". В главу включались четыре состава:

- **неправомерное проникновение в автоматизированную компьютерную систему или сеть (ст. 207);**
- **введение в компьютерную систему или сеть заведомо ложной информации (ст. 268);**
- **распространение вирусных программ (ст. 269);**
- **нарушение правил, обеспечивающих безопасность и сохранность информации компьютерной системы или сети (ст. 270).**

[1] *Курушин В. Д., Минаев В. А.* Указ. соч. С. 129.

Однако в дальнейшем в силу замечаний, высказанных как теоретиками уголовного права, так и практиками в области компьютерных технологий, предлагавшиеся составы были объединены в три статьи, которые в настоящий момент и представлены в главе 28 УК РФ.

В то же время борьба с компьютерными преступлениями не исчерпывается только разработкой и применением уголовно-правовых норм. В связи **с этим в литературе сложились различные мнения о приоритетности имеющихся в распоряжении государства мер воздействия на данную группу общественных отношений.**

По мнению одной группы авторов (это касается представителей зарубежной науки, например, большинства американских исследователей), наиболее эффективными методами борьбы являются лишь тщательно продуманные организационные и технологические приемы защиты, обеспечивающие как "физическую" безопасность компьютеров (от разрушения, повреждения и т. п.), так и безопасность осуществляемых на них процессов обработки информации на всех уровнях, начиная с ввода исходных данных и кончая обработкой полученных результатов. В связи с этим указанные авторы весьма скептически относятся к возможностям общепревентивного воздействия уголовного наказания как средства борьбы с компьютерными преступлениями, поскольку доходы от преступлений, связанных с компьютерами, часто оказываются попросту фантастическими, а вероятность разоблачения преступников — чрезвычайно мала[1].

Другая группа авторов (российские ученые, например, А. П. Курило, В. Д. Аносов, Л. М. Ухлинов, В. Д. Курушин, В. А. Минаев и др.) считает, что борьба с компьютерной преступностью должна осуществляться комплексно, путем применения согласованных правовых норм, на основе методов авторского, патентного, гражданского, уголовного и административного права, специального законодательства, охватывающего проблему информационной безопасности; при их технологической и организационной поддержке[2].

---

[1] *Никифоров В. С., Решетников Ф. М.* Современное уголовное право. М.: Наука, 1990. С. 192.

[2] *Курило А. П.* Указ. соч. С. 9; *Аносов В. Д., Ухлинов Л. М.* Об основных направлениях государственной политики в области борьбы с компьютерной преступностью // Вестник Российского общества информатики и вычислительной техники. 1997. № 4. С. 6—12.

Следует отметить, что в соответствии с поручением Президента РФ и предложениями Совета Безопасности РФ ФСБ, МВД, Генеральной прокуратурой, Министерством юстиции, Верховным Судом, Миноборонпромом и другими заинтересованными министерствами и ведомствами России разрабатывается Федеральная программа "Борьба с компьютерной преступностью", которая предусматривает создание эффективных мер по выявлению и пресечению преступлений с использованием возможностей средств вычислительной техники, разработку нормативной базы, касающейся административной и уголовной ответственности за компьютерные преступления; подготовку соответствующих специалистов[1].

Проект Программы борьбы с компьютерной преступностью представляет собой достаточно полный и целостный документ, охватывающий как технические, так и правовые вопросы, и предлагающий комплексный подход к решению поставленной проблемы, задействуя при этом силы и средства различных министерств и ведомств. В настоящее время над различными аспектами данной проблемы работают:

- правоохранительные органы, наделенные правом проведения оперативно-розыскной деятельности — ФСБ и МВД. При этом в рамках указанных правоохранительных органов к настоящему времени созданы специальные подразделения по борьбе с компьютерными преступлениями. Проблема стала осознаваться настолько остро, что Академией МВД в 1999 г. произведен набор двух групп слушателей численностью по 50 человек для обучения "хакерскому ремеслу" и методам их выявления и обезвреживания;
- специальные службы и силовые экономические ведомства, наделенные правом проведения оперативно-розыскных мероприятий, в ходе которых им становятся известны факты подготовки и реализации компьютерных преступлений; органы суда и прокуратуры;
- ведомства и организации, разрабатывающие, сертифицирующие и производящие средства защиты информации (Гостехкомиссия РФ, ФАПСИ, Миноборонпром);

[1] *Никитенко Н. И.* Актуальные проблемы выявления и раскрытия компьютерных преступлений // Вестник Российского общества информатики и вычислительной техники. 1997. № 4. С. 22—23.

- органы государственного управления, обеспечивающие контроль за качеством работы средств и систем защиты, а также работой самих служб информационной безопасности на объектах защиты (Гостехкомиссия РФ, ФАПСИ, ФСБ);
- сами службы информационной безопасности, являющиеся основным звеном, обеспечивающим поддержку необходимого уровня безопасности информации на объекте защиты и выступающие в качестве основного интегрирующего звена в проблеме борьбы с компьютерной преступностью.

В связи с изложенным к числу первоочередных мер, направленных на выявление, пресечение, раскрытие, предупреждение и профилактику компьютерных преступлений, отнесены следующие:

- создание в рамках правоохранительных органов организационных структур, способных вести эффективную борьбу с компьютерной преступностью, а также осуществлять контроль за эффективностью выявления, предупреждения и пресечения таких правонарушений; организация взаимодействия правоохранительных органов, специальных служб, судебной системы, обеспечение их необходимой материально-технической базой и программно-техническим инструментарием;
- разработка системы предупреждения правонарушений, осуществляемых в сфере компьютерной информации; организация системы их статистического учета;
- организация эффективного взаимодействия общественных и частных организационных структур (фондов, ассоциаций, фирм, служб безопасности финансовых, банковских и коммерческих структур), осуществляющих практические мероприятия по обеспечению безопасности и защите информации, обрабатываемой в электронной форме, с государственными структурами (МВД, ФСБ, ФАПСИ и др.);
- создание системы обучения, подготовки, переподготовки специалистов правоохранительных органов, органов суда и прокуратуры в области борьбы с компьютерными преступлениями;
- организация взаимодействия правоохранительной системы РФ с международными организациями и национальными правоохранительными органами зарубежных стран, ведущими борьбу с проявлениями компьютерной преступности;

- информирование населения о возможных последствиях компьютерных преступлений; привлечение СМИ к отображению и анализу правонарушений в информационной сфере;
- формирование целостной взаимосвязанной системы мер правового характера, что предполагает:

— определение роли и места правовых мер в системе борьбы с данными видами преступлений; содержания этих правовых мер (не ограничиваясь только уголовно-правовыми мерами); критериев, по которым можно было бы разграничить деяния, влекущие административную или уголовную ответственность, конкретизировать квалифицирующие признаки, привести в соответствие назначаемые виды наказаний и тяжесть совершенных преступлений, их общественную опасность; механизма реализации законопроектов, в которых следует определить круг субъектов данного вида деятельности, их правовой статус, принятие соответствующих стандартов, правил пользования и др.;

— разработку и внесение в УПК, ГК, КоАП изменений и дополнений в части, касающейся проблем выявления, расследования, пресечения, доказательства правонарушений в сфере компьютерной информации;

— создание законодательной базы, регламентирующей сбор, регистрацию и использование в суде в качестве доказательств данных, полученных в результате проведения оперативно-технических мероприятий при расследовании компьютерных правонарушений;

— подготовку методических материалов по расследованию компьютерных преступлений для правоохранительных органов, прокуратуры и суда, в том числе по применению: специальных технических средств и методов выявления компьютерных преступлений, методов составления психологического и профессионального портрета предполагаемого преступника по оставленным следам, по серийным компьютерным преступлениям, информационно-поисковых моделей для банка данных по компьютерным преступлениям и др.;

— обеспечение защиты интересов и восстановление прав субъектов, ставших жертвами компьютерных преступлений[1].

[1] *Масалов А. В.* Правовые основы предотвращения компьютерных преступлений // Вестник Российского общества информатики и вычислительной техники. 1997. № 4. С. 17—20.

По мере развития телекоммуникационных технологий и их распространения в РФ угроза компьютерной преступности все в большей степени будет затрагивать интересы национальной безопасности РФ. Поэтому от того, в какой степени в обществе будет осознана угроза компьютерной преступности, от эффективности мер противодействия этому негативному явлению на начальном этапе организации деятельности правоохранительной системы будет зависеть состояние информационной и национальной безопасности России в целом.

В данном учебном пособии рассматриваются понятие и уголовно-правовая характеристика состава преступления, предусмотренного ст. 272 УК РФ “Неправомерный доступ к компьютерной информации”.

УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

1. Объект неправомерного доступа к компьютерной информации

Общим объектом преступлений в сфере компьютерной информации является совокупность всех общественных отношений, охраняемых уголовным законом.

При определении **родового объекта** необходимо исходить из места расположения главы УК РФ, посвященной данному виду преступлений. Глава 28 УК РФ помещена в раздел 9 УК РФ "Преступления против общественной безопасности и общественного порядка". Тем самым законодатель определил объект посягательства преступлений в сфере компьютерной информации как отношения общественной безопасности. Однако преступления в сфере компьютерной информации посягают не на все отношения общественной безопасности в целом, а лишь на одну из ее сторон, связанную с информационной безопасностью. Такое уточнение является необходимым ввиду того, что отношения безопасности разнообразны и многогранны, поскольку включают в себя государственную, общественную, оборонную, экологическую, продовольственную и другие направления безопасности.

Существует два основных подхода к понятию информационной безопасности.

Первый подход строится на оценке понятия информационной безопасности как широкого явления, составной частью которого является защита информации.

Например, М. В. Арсентьев считает, что **информационная безопасность** — это снятие информационной неопределенности

относительно объективно и субъективно существующих реальных и потенциальных угроз за счет контроля над мировым информационным пространством и наличия возможностей, условий и средств для отражения этих угроз, что в совокупности определяет уровень (степень) информационной безопасности каждого субъекта[1].

Другая группа ученых связывает информационную безопасность с защитой информации. При этом в рамках данного подхода понятие информационной безопасности трактуется поразному. Например, В. Ю. Статьев, В. А. Тиньков определяют **информационную безопасность** как защиту информации и поддерживающей ее инфраструктуры с помощью совокупности программных, аппаратно-программных средств и методов, а также организационных мер, с целью недопущения причинения вреда владельцам этой информации или поддерживающей его инфраструктуре[2].

По мнению Феоктистова Г. Г., информационная безопасность — получение максимальной информации о намерениях и потенциальных действиях своих оппонентов и минимальная утечка информации о своих планах. Она включает комплекс мер и совокупность действий, направленных на защиту собственных источников информации, каналов ее передачи и создание системы дезинформации[3]. В данных определениях автор акцентирует внимание на информационной безопасности в ее узком смысле. (Ранее применительно к данному вопросу использовался термин "защита информации".) Кроме того, последнее из указанных определений носит социологический характер и не увязывается с нормами закона, регулирующего отношения информационной безопасности.

Урсул А. Д. определяет информационную безопасность как состояние защищенности основных сфер жизнедеятельности по отношению к опасным информационным воздействиям[4].

---

[1] *Арсентьев М. В.* К вопросу о понятии "информационная безопасность" // Информационное общество. 1997. № 4—6. С. 50.

[2] *Статьев В. Ю., Тиньков В. А.* Информационная безопасность распределенных информационных систем // Информационное общество. 1997. № 1. С. 68.

[3] *Феоктистов Г. Г.* Информационная безопасность общества // Социально-политический журнал. 1996. № 5. С. 211—212.

[4] *Урсул А. Д.* Информационная стратегия и безопасность в концепции устойчивого развития // НТИ. Сер. 1. Орг. и методика информ. работы. 1996. № 1. С. 7.

Или, например, информационная безопасность — состояние защищенности информационной среды общества; состояние либо отсутствие информационных угроз, либо, при наличии таковых, состояние защищенности и, следовательно, устойчивости основных сфер жизнедеятельности и др.[1]

Указанные определения в большей степени соответствуют положениям действующего законодательства, анализ которого приводится далее.

В основе содержания понятия **информационная безопасность** лежит понятие безопасность. В соответствии со ст. 1 Федерального закона "О безопасности"[2] **безопасность** — состояние защищенности жизненно важных интересов личности общества, государства от внутренних и внешних угроз.

Основные объекты безопасности: **личность, ее права и свободы; общество — его материальные и духовные потребности; государство — его конституционный строй, суверенитет и территориальная целостность.**

С учетом изложенного информационную безопасность **можно определить как состояние защищенности жизненно важных интересов личности, общества, государства в информационной сфере от внешних и внутренних угроз.**

Согласно ст. 2 Федерального закона "О международном информационном обмене" **информационная сфера (среда)** — сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации[3].

Таким образом, **информационная безопасность** — состояние защищенности жизненно важных интересов личности, общества, государства в информационной (сфере) среде от внешних и внутренних угроз, обеспечивающее ее формирование, использование и развитие в интересах граждан, общества, государства (т. е. в дальнейшем речь будет идти об информационной безопасности в узком смысле слова).

Достоинство указанного определения заключается в том, что оно строится на необходимости учета и согласования интересов трех основных субъектов, функционирующих в информа-

[1] *Арсентьев М. В.* Указ. соч. С. 49.
[2] Закон РФ "О безопасности" // Ведомости съезда народных депутатов РФ и Верховного Совета РФ. 1992. № 15. Ст. 769.
[3] Федеральный закон "Об участии в международном информационном обмене" // Собрание законодательства РФ. 1996. № 28. Ст. 3347.

ционной сфере, — личности, общества и государства, а также расширения границ традиционного рассмотрения проблем защиты информации в системах передачи информации и телекоммуникациях.

Одним из важнейших аспектов содержания понятия информационная безопасность являются определение, анализ и классификация возможных угроз безопасности.

Согласно ст. 3 Федерального закона "О безопасности" угроза безопасности — совокупность условий и факторов, создающих опасность жизненно важным интересам.

В литературе приводятся различные классификации угроз безопасности[1]. Среди них можно выделить следующие:

1. По источнику угрозы:

- **внешние** — угрозы, связанные со стихийными бедствиями, техногенными, политическими, социальными факторами, развитием информационных и коммуникационных технологий, другими внешними воздействиями;
- **внутренни**е — угрозы, связанные с отказами вычислительной и коммуникационной техники, ошибками программного обеспечения.

2. По природе возникновения:

- **естественные (объективные)** — угрозы, вызванные воздействием на информационную среду объективных физических процессов или стихийных природных явлений, не зависящих от воли человека;
- **искусственные (субъективные)** — угрозы, вызванные воздействием на информационную сферу человека.

Среди искусственных угроз выделяют:

- **непреднамеренные (случайные) угрозы** — ошибки программного обеспечения, персонала, отказы вычислительной и коммуникационной техники и т. д.;
- **преднамеренные (умышленные) угрозы** — неправомерный доступ к информации, разработка специального программного обеспечения, используемого для осуществления неправомерного доступа, разработка и распространение вирусных про-

[1] *Охрименко С. А., Черней Г. А.* Угрозы безопасности автоматизированным информационным системам (программные злоупотребления) // Научно-техническая информация. Сер. 1. Орг. и методика инф. работы. 1996. № 5. С. 5—13.

грамм и т. д. Преднамеренные угрозы обусловлены действиями людей и ориентированы на неправомерное нарушение конфиденциальности, целостности и/или доступности информации, а также использование ресурсов в своих целях.

3. По принципу воздействия: с использованием доступа; с использованием скрытых каналов.

4. По цели реализации: нарушение конфиденциальности; нарушение целостности; нарушение доступности.

5. По характеру воздействия: активные; пассивные.

6. По объекту воздействия: угрозы, воздействующие на информационную среду в целом; угрозы, воздействующие на отдельные ее элементы.

7. По способу воздействия на объект атаки: непосредственно воздействующие на объект атаки; воздействующие на систему разрешений; воздействующие опосредованно и т. д.

Кроме того, в литературе на основании данных статистики предпринята попытка ранжирования основных угроз по степени их опасности **(с учетом вероятности их проявления и стоимости ликвидации последствий):**

- несанкционированный доступ (на первом месте);
- пожары;
- умышленное нарушение нормальной работы (заражение вирусами, умышленный ввод искаженных данных, умышленный вывод из строя оборудования и его хищение) — в статистике некоторых стран указанная угроза находится на втором месте;
- использование программного обеспечения, содержащего ошибки[1].

Таким образом, основные проблемы информационной безопасности связаны прежде всего с умышленными угрозами (действиями людей), так как именно они являются основной причиной и движущей силой преступлений и нарушений. В то же время, средства вычислительной техники (прежде всего ЭВМ), встраиваясь в систему отношений по поддержанию общественной безопасности, оказывают на них определенное воздействие. В некоторых случаях ЭВМ функционируют как источники повышенной опасности, и тогда нарушение установ-

[1] *Герасименко В. Г., Сергеев В. В.* Информационная безопасность в банках США и Великобритании // Банковское дело. 1996. № 7. С. 30.

ленных правил их эксплуатации может привести к нарушению общественной безопасности.

С учетом изложенного в данной работе рассматривается только **один из видов преднамеренных угроз информационной среде — неправомерный доступ к компьютерной информации.** Согласно статистике наибольшую опасность представляет несанкционированный (неправомерный) доступ к компьютерной информации. Ежегодные потери от указанного преступления, например американского бизнеса, за последние 10 лет возросли в 1000 раз и составили по данным на середину 1996 г. около 150—300 млрд. долл. (приблизительно 10% валового национального продукта США)[1].

В литературе нет единства мнения и по поводу определения **видового объекта** ст. 272 УК РФ.

Некоторые авторы (например, Бородин С. В., Полубинский С. В.[2]) полагают, что **видовым (групповым) объектом** для преступлений главы 28 УК РФ является совокупность охраняемых уголовным законом интересов в области безопасности изготовления, использования и распространения компьютерной информации, информационных ресурсов, информационных систем и технологий либо права и интересы физических и юридических лиц, общества и государства по поводу использования автоматизированных систем обработки данных.

Однако при таком подходе объект посягательства отождествляется с конкретным социальным благом, которому наносится ущерб и которое составляет содержание общественных отношений, охраняемых нормами главы 28 УК РФ.

Большинство же авторов (Ляпунов Ю., Максимов В., Батурин Ю., Скоромников К., Комиссаров В., Ткачевский Ю., Кузнецова Н. и др.) с учетом положений ст. 1 Федерального закона "Об информации, информатизации и защите информации" считают, что **видовым объектом** является совокупность общественных отношений, обеспечивающих безопасность компьютерной информации, т. е. правомерное и безопасное изготовление, распространение и использование компьютерной информации, а также информационных систем, информационных

[1] *Герасименко В. Г., Сергеев В. В.* Указ. соч. С. 28.
[2] Российское уголовное право. Особенная часть / Под ред. *В. Н. Кудрявцева, А. В. Наумова.* М.: Юрист, 1997. С. 347.

ресурсов, информационных технологий и средств их обеспечения. Аналогичный вывод следует и из заглавия гл. 28 УК РФ — "Преступления в сфере компьютерной информации"[1].

При этом некоторые из них, например Батурин Ю., Жодзишский А., Сюнтюренко О., Колочков Ю., употребляют в связи с этим термин "компьютерная безопасность"[2].

Такая позиция, на наш взгляд, более удачна ввиду того, что УК РФ содержит большое количество составов преступлений, которые можно отнести к категории информационных.

Уяснение особенностей видового (группового) объекта важно для того, чтобы отграничить преступления, предусмотренные гл. 28 УК РФ, от других, связанных с использованием ЭВМ, системы ЭВМ или их сети для совершения других преступлений. В частности, неправомерный доступ к компьютерной информации может выступать как один из этапов для совершения других преступлений, например, неправомерный доступ к информации, составляющей государственную тайну, с целью государственной измены; неправомерный доступ и копирование программ для ЭВМ (объектов авторского права). В этих случаях квалификация будет проводиться по совокупности соответствующих составов. Таким образом, преступления в сфере компьютерной информации, и прежде всего неправомерный доступ к ней, могут нанести ущерб нескольким объектам уголовно-правовой охраны. То есть, посягая на основной объект, они посягают и на дополнительный объект, поражая блага более конкретного свойства: личные права и неприкосновенность частной сферы, имущественные права и интересы, общественную и государственную безопасность и конституционный строй. Поэтому отношения, связанные с охраной указанных благ, выступают в качестве дополнительного объекта компьютерных преступле-

---

[1] *Ляпунов Ю., Максимов В.* Указ. соч. С. 9; *Скоромников К. С.* Неправомерный доступ к компьютерной информации и его расследование // Прокурорская и следственная практика. 1998. № 1 С. 168; Уголовное право РФ. Особенная часть: Учебник / Под ред. *Г. Н. Борзенкова* и *В. С. Комиссарова.* М.: Олимп; Изд-во АСТ, 1997. С. 537; Новое уголовное право России. Особенная часть: Учебное пособие. М.: Зерцало, Теис, 1996. С. 274.

[2] *Батурин Ю. М., Жодзишский А. М.* Компьютерные правонарушения: криминализация, квалификация, раскрытие // Сов. государство и право. 1990. № 12. С. 89; *Сюнтюренко О. В., Колочков Ю. М.* Проблемы правового обеспечения защиты информации и компьютерной безопасности // Научно-техническая информация. Сер. 1. Орг. и методика инф. работы. 1996. № 8. С. 9.

ний. При этом дополнительный объект, как правило, является более ценным, чем основной. Это отражено и в названии гл. 28 УК, которое говорит не о посягательстве на объект, а о посягательствах в определенной "сфере". Отсутствие посягательства на эти общественные отношения (либо незначительность такого посягательства) исключает уголовную ответственность в силу ч. 2 ст. 14 УК. Например, кратковременное использование без разрешения чужого игрового компьютера является неправомерным доступом к компьютерной информации и, следовательно, в полной мере поражает основной объект преступления, но не поражает дополнительного, т. е. не содержит необходимого признака состава преступления (если это, конечно, не связано, например, с незаконным проникновением в жилище).

Что касается **непосредственного объекта**, то его можно определить исходя из диспозиции ст. 272 УК РФ.

При этом в оценке непосредственного объекта ситуация аналогична оценке видового объекта.

Одна группа ученых (Клепицкий И. А., Пашин С. А. и др.) понятие непосредственного объекта определяют через категории права или интереса собственника (владельца) ЭВМ, системы ЭВМ или сети ЭВМ на неприкосновенность содержащейся в ней информации[1].

Другая группа ученых (Скоромников К. С. и др.) отождествляют **непосредственный и видовой объекты,** определяя непосредственный объект как общественные отношения по обеспечению информационной безопасности[2].

Очевидно, что такой подход является не совсем верным, к тому же по степени охвата охраняемых общественных отношений — очень широким.

Более верен подход тех авторов (например, Бородин С. В., Полубинский С. В., Ваулина Т. И.), которые определяют непосредственный объект ст. 272 УК РФ как отношения, обеспечивающие безопасность компьютерной информации, так как непосредственный объект всегда находится в группе общественных

[1] Уголовное право России. Особенная часть: Учебник / Отв. ред. *В. В. Здравомыслов*. М.: Юристъ, 1996. С. 352; Комментарий к Уголовному кодексу РФ. Особенная часть / Под общ. ред. *Ю. И. Скуратова* и *В. М. Лебедева*. М.: Инфра-М—НОРМА, 1996. С. 411.

[2] Пособие для следователя. Расследование преступлений повышенной общественной опасности. С. 338.

отношений, обособляемых под наименованием родового объекта преступления[1].

Таким образом, с учетом вышеизложенного, положений Закона РФ "О безопасности" и Федерального закона "Об информации, информатизации и защите информации", а также диспозиции ст. 272 УК РФ можно определить **непосредственный объект** как отношения, обеспечивающие безопасность (неприкосновенность) компьютерной информации, а также безопасную (нормальную) эксплуатацию (работу) ЭВМ, системы ЭВМ или их сети.

В качестве **дополнительного объекта** ст. 272 УК могут выступать общественные отношения, охраняющие права собственника (владельца) компьютерной информации на ее неприкосновенность, а также интересы относительно правильной (безопасной) эксплуатации ЭВМ, системы ЭВМ или их сети.

Опасность неправомерного доступа к компьютерной информации заключается в том, что в результате его совершения могут наступить самые разнообразные последствия: нарушение интеллектуальной собственности, разглашение сведений, составляющих государственную, коммерческую тайну, разглашение сведений о частной жизни граждан, имущественный ущерб в виде прямых убытков и неполученных доходов, потеря репутации фирмы и т. д. Опасность данного преступления многократно возрастает, когда преступник получает доступ к автоматизированным системам, обслуживающим сферу национальной обороны, атомной энергетики, транспорта, связи, медицины, торговли, денежного обращения и т. д. Причем в ряде случаев все возможные последствия такого доступа заранее неизвестны преступнику. Даже разработчики компьютерной техники или программного обеспечения не могут предусмотреть всех возможных ситуаций, которые возникают в процессе их функционирования, тем более если это касается умышленных преступных действий.

Опасность неправомерного доступа определяется также и степенью его распространенности в обществе и более высокой

[1] Уголовное право. Особенная часть: Учебник для вузов / Отв. ред.: *И. Я. Козаченко, З. А. Незнамова, Г. П. Новоселов.* С. 557; Российское уголовное право. Особенная часть / Под ред. *В. Н. Кудрявцева, А. В. Наумова.* С. 348.

степенью латентности по сравнению с другими преступлениями в сфере компьютерной информации. По статистике зарубежных стран, например США, около 85% случаев несанкционированного доступа к информационным системам остаются нераскрытыми[1].

Распространенность данного преступления обусловлена прежде всего расширением сферы применения средств вычислительной техники, ростом уровня доверия к автоматизированным системам обработки информации. Средствам вычислительной техники доверяют все более сложную и ответственную работу, от качества выполнения которой зависит жизнь и благосостояние людей. ЭВМ управляют технологическими процессами на предприятиях и атомных электростанциях, движением самолетов и поездов, выполняют финансовые операции, обрабатывают секретную и конфиденциальную информацию. С другой стороны, как отмечалось ранее, неправомерный доступ выступает в качестве одного из этапов совершения других преступлений, он "удобен" в силу своей скоротечности, обезличенности, отсутствия непосредственного контакта с объектами, которым наносится ущерб, и т. д.

Например, 4 из 5 компьютерных преступлений, расследовавшихся ФБР (США), имели отношение к неправомерному доступу[2].

Что касается России, то по заявлению заместителя начальника управления по борьбе с экономическими преступлениями МВД РФ в период с 1994 по 1996 г. российские компьютерные преступники совершили более 500 попыток проникновения в компьютерные сети только одного Центрального банка и сумели похитить оттуда около 250 млрд. рублей[3].

Однако точной статистики по данному виду преступлений не ведется, поэтому данные о размахе этого посягательства носят весьма вероятностный характер.

---

[1] *Селиванов Н.* Указ. соч. С. 36.

[2] Реальные преступления в виртуальном мире // Жизненное пространство. 1997. № 12. С. 23.

[3] *Анин В.* Наиболее серьезные нарушения в области информационной безопасности в 1996 году // Конфидент. 1997. № 6. С. 49.

2. Предмет неправомерного доступа к компьютерной информации

Согласно диспозиции ст. 272 УК РФ предметом рассматриваемого состава является **охраняемая законом компьютерная информация, то есть информация на машинном носителе, в ЭВМ, системе ЭВМ или их сети.**

Однако, прежде чем говорить о компьютерной информации, необходимо определить, что такое информация вообще.

Несмотря на кажущуюся простоту этого понятия, уяснение сущности понятия "информация" имеет определенные сложности, так как в литературе, законодательстве, в обиходной речи трактуется неоднозначно.

Первоначально, приблизительно до 40-х гг. XX в., термин "информация" и в обиходе, и в научной литературе рассматривался в качестве синонима таких понятий, как сведения, сообщения, сигнал. И как таковое понятие информации изучалось в теории передачи сообщений и употреблялось в обиходной речи, в литературе. Кроме того, была широко распространена точка зрения, что информация как нечто неосязаемое и нематериальное не имеет прямого отношения к экономике. Само понятие и содержание информации трактовалось довольно упрощенно — она рассматривалась как некая реалия, объективно существующая наряду с материальными вещами или в самих вещах[1].

Такое ее понимание было обусловлено установившимися языковыми штампами, как, например, когда по аналогии с обменом веществ говорят об обмене информацией, о ее хищении, продаже и т. д. В данном случае информация рассматривается как самостоятельная субстанция, которая в процессе передачи отрывается от того предмета, которому она передается, т. е. информация может быть передана, если она носит предметный характер. Данный подход не дает возможности определить: содержанием чего является информация, какова ее природа и материальная основа возникновения.

Однако с развитием технических средств передачи сведений и особенно с изобретением компьютеров, позволяющих ре-

[1] *Батурин Ю. М.* Проблемы компьютерного права. С. 14—15.