Федеральное агентство по образованию

Государственное образовательное учреждение
высшего профессионального образования

Владимирский государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА
ОБЪЕКТОВ ИНФОРМАЦИИ

КНИГА 17

М.Ю. МОНАХОВ, В.Ф. ТАШМУХАМЕДОВА

ЗАЩИТА АВТОРСКИХ ПРАВ НА ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Актуальные вопросы информационного права

Учебное пособие

Владимир 2009

УДК 930.1
ББК 32.81
М77

Редактор серии – доктор технических наук М.Ю. Монахов

Рецензенты:
Кандидат технических наук, доцент
зав. кафедрой оперативно-технической деятельности
Владимирского юридического института
Федеральной службы исполнения наказаний
К.Н. Курысев

Кандидат технических наук, доцент
Владимирского государственного университета
А.Б. Градусов

Печатается по решению редакционного совета
Владимирского государственного университета

Монахов, М. Ю.

М77 Защита авторских прав на программное обеспечение : актуальные вопросы информационного права : учеб. пособие / М. Ю. Монахов, В. Ф. Ташмухамедова ; Владим. гос. ун-т. – Владимир : Изд-во Владим. гос. ун-та, 2009. – 59 с. (Комплексная защита объектов информатизации. Кн. 17). – ISBN 978-5-89368-999-0.

Это семнадцатая книга из серии «Комплексная защита объектов информатизации». В ней представлен систематизированный материал по основным методам и средствам защиты авторских прав на программное обеспечение. Пособие отражает современный подход к защите авторского права на программное обеспечение.

Предназначено для студентов специальности 090104 «Комплексная защита объектов информатизации» дневной формы обучения.

Библиогр.: 35 назв.

УДК 930.1
ББК 32.81

ISBN 978-5-89368-999-0

ПРЕДИСЛОВИЕ

Защита авторского права на программное обеспечение один из наиболее актуальных вопросов гражданского права.

Определений программы и заменяющих ее терминов довольно большое количество, в мире нет устоявшейся терминологии на сей счет. Отечественное законодательство использует термин «программа для ЭВМ» и понимает под последней форму представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата. Также для целей закона в программу включаются подготовительные материалы, полученные в ходе ее разработки, и порождаемые ею аудиовизуальные отображения. Включение подготовительных материалов в определение программы позволяет обойти ряд спорных моментов (например, подлежит ли правовой охране программа, написанная на языке высокого уровня, которая не может непосредственно восприниматься компьютером).

Определение законодателя, конечно, спорное и сам термин «программа для ЭВМ» в принципе устаревший. Уже редко где в современной литературе встретишь слово ЭВМ, а вместо слова «программа» чаще используют термины «программный продукт» и «программное обеспечение».

Для целей данной работы мы будем использовать термины «программное обеспечение», «программный продукт» и «программа» как синонимы, понимая под последними любые компьютерные программы.

У программы как коммерческого продукта существует другая часть - носитель (дискета, компакт-диск, DVD и т.п.), печатная документация и красочная упаковка. Для выделения основной части программы, представляющей из себя последовательный набор команд, мы будем использовать термин «код». Сразу оговоримся, что под программой понимают и программы, написанные на языке програм-

мирования (в форме исходных кодов), и программы, представленные на машинном языке (в форме объектных кодов). Исходный код (исходный текст) представляет по сути алгоритм, написанный на удобном для человека языке, который при помощи специализированных программ преобразуется в объектный код, понятный компьютеру.

Обратное преобразование от объектного кода к исходному в общем случае невозможно (хотя отдельные части программы возможно перевести на язык, понятный человеку). Для обозначения этого обратного преобразования законодатель использует термин «декомпилирование программы».

Отметим, что программы, написанные на различных языках программирования, могут давать один и тот же объектный код, как, впрочем, один и тот же исходный текст в зависимости от конкретного компьютера и программы трансляции может иметь различный машинный вид.

Исходные тексты программ, как правило, держатся производителями в секрете. Такие популярные программы, как Microsoft Word, распространяются исключительно в объектном виде.

Хотелось бы обозначить еще одну группу терминологических проблем. Они связаны с тем, что понимание некоторых важных терминов в законе и на практике существенно различно.

Во-первых, это вопрос, связанный с обычным пониманием терминов «программа» и «экземпляр программы» в качестве синонимов. С точки зрения законодательства - это принципиально различные вещи. Так, экземпляр программы, записанный на неком носителе, можно приобрести по договору купли-продажи. Программу же купить нельзя в силу ее нематериальной природы. Можно лишь приобрести права на ее использование. Разница между экземпляром программы и программой такая же, как разница между книгой и литературным произведением.

Также термины «использование» и «пользователь» в законе принципиально отличаются от их устоявшейся трактовки на практике. Так, в законе под использованием программы понимается выпуск в свет, воспроизведение, распространение и иные действия по ее введению в хозяйственный оборот (в том числе в модифицированной фор-

ме). Соответственно пользователями будут издательства, распространители программ, предприятия, осуществляющие тиражирование и т.д. Так называемые конечные пользователи (users), т.е. лица, которые пользуются программой по ее прямому назначению, пользователями в смысле закона не являются. Точнее, они являются пользователями компьютера, а не программы.

Сегодня программы для персонального компьютера, вопреки воли их правообладателей, можно практически за бесценок приобрести в легально существующих магазинах. В чем же дело? Существуют международные соглашения по охране результатов интеллектуальной деятельности, в которых участвует Российская Федерация; существует российское законодательство, относящееся к защите интеллектуальной собственности; есть даже статья 146 Уголовного кодекса РФ, устанавливающая ответственность для тех, кто нарушает авторские права.

Однако так называемые «пиратские» диски продаются. Отметим, что проблема незаконного использования программ не является чисто российской. Масштабы незаконного использования программного обеспечения во всем мире огромны. С одной стороны, общественная мораль не признает существенную часть подобных действий преступными, с другой – довольно убедительно звучит мнение, что повсеместное нарушение закона свидетельствует о его несоответствии реальным общественным отношениям. Возможно, закон не верен по сути, а возможно, общество еще не готово к исполнению этого закона. На наш взгляд, бессмысленно запрещать то, что в обществе считается нормой. Следует сначала достигнуть определенного общественного согласия.

Представляется, что если закон делает правонарушителями значительную часть законопослушных граждан, то неважно, какими благими целями прикрываются его сторонники. Такой закон лишь подрывает уважение к государству, он способствует злоупотреблениям и коррупции и несовместим с принципами демократического общественного устройства.

Итак, какие же правовые институты могут использоваться для охраны программного обеспечения.

Этих институтов три и все они относятся к категории так называемой «интеллектуальной собственности». Название «интеллектуальная собственность» отражает не то, что права на результаты интеллектуальной деятельности - это отдельная разновидность права собственности, как например частная или муниципальная собственность. Название говорит лишь о том, что понятие интеллектуальной собственности является заменой (аналогом) праву собственности для нематериальных объектов.

Смысл прав интеллектуальной собственности заключается в том, что их обладатель вправе требовать от других лиц воздерживаться от любого использования принадлежащих ему результатов интеллектуальной деятельности. Такие абсолютные права получили название исключительных прав.

Как отмечают многие специалисты, для защиты программ могут быть использованы как минимум три института. Это институты авторского права, патентного права и коммерческой тайны. Авторское право является основным и наиболее разработанным институтом охраны программ.

Глава 1. ЭТАПЫ СТАНОВЛЕНИЯ И РАЗВИТИЯ АВТОРСКОГО ПРАВА НА ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Введение

Новизна и динамизм общественных отношений, порожденных научно-технической революцией в сфере информационных технологий, осложняет теоретическое осмысление соответствующих правовых аспектов. Развитие правовых институтов компьютерного права - результат дискуссий и компромиссов между учеными и практиками, сторонниками различных точек зрения на данную проблему. Дискуссия полностью не завершена и к настоящему моменту, и это оказывает свое влияние на развитие законодательства.

Одним из основных аспектов дискуссии является вопрос правовой природы компьютерных программ и баз данных как объектов права. В отечественной и зарубежной литературе могут быть выделены три основные точки зрения на возможности правовой защиты программных средств как специфического объекта интеллектуальной собственности:

- использование правовых институтов авторского права;
- патентная защита;
- создание специальных правовых институтов защиты.

Законодательство России вслед за законодательством большинства промышленно развитых стран предусматривает использование в качестве основного правового института защиты компьютерных программ и баз данных правовые институты авторского права.

В главе дается историческая ретроспектива становления законодательной базы авторского права на программное обеспечение как в мире в целом, так и на территории России в частности.

1.1. Международная история развития авторского права на программное обеспечение

Впервые в мире программа для ЭВМ в качестве объекта правовой охраны была зарегистрирована в ноябре 1961 г. в США (Регистр США по авторскому праву циркуляр 61).

В 1971 г. проблематика защиты компьютерных программ впервые приобрела межгосударственный характер - консультационной группой Всемирной организации интеллектуальной собственности (ВОИС) были рассмотрены вопросы целесообразности и возможности такой защиты. В середине семидесятых годов данная проблема параллельно рассматривалась двумя авторитетными международными организациями - ВОИС и Международной ассоциацией промышленной собственности (АИППИ).

В 1975 г. конгресс АИППИ в Сан-Франциско принял решение рекомендовать использовать для охраны программного продукта возможности национального законодательства стран участниц, прежде всего в форме авторского права. Подразумевалось, что такое положение должно сохраниться вплоть до выработки специальных международных норм защиты интеллектуальной собственности в сфере программно-математического и информационного обеспечения ЭВМ.

Следующим знаменательным событием было принятие ВОИС в 1978 г. Типовых положений по охране программного обеспечения вычислительных машин, состоящих из десяти разделов, суммирующих позитивный опыт постановки и решения проблем в сфере правовой охраны программного обеспечения, накопленный к данному моменту в различных странах. В качестве основных вопросов, рассматриваемых в Положениях, следует упомянуть определение следующих понятий:

- основные термины;
- основные права на программное обеспечение;
- условия возникновения прав;
- сроки действия прав;
- условия, размер и порядок компенсаций.

В качестве следующего шага предполагались подготовка и заключение соответствующего многостороннего международного договора об охране программного обеспечения. Однако жизнь внесла свои коррективы – данное намерение так и не было реализовано. Причиной послужило принятие поправок к национальному законодательству об авторских правах, осуществленное в большинстве промышленно развитых стран в начале 80-х годов. Данные поправки модернизировали

действующее законодательство, сделав его относительно приемлемым на текущий момент для адекватной правовой охраны программных разработок. В результате вопрос разработки специального международного законодательства потерял актуальность и был снят с повестки дня международных организаций. Охрана прав авторов программ обеспечивается в соответствии с нормами Всемирной (Женевской) и Бернской конвенций. Тем не менее, роль Положений не следует неоправданно занижать, так как они имели определенное методическое значение при модернизации национальных законодательств, в частности, при определении терминов и понятий.

Разработка международных многосторонних договоров в сфере охраны программного обеспечения значительно осложняется наличием проблемы согласования интересов государств, обладающих различной степенью научно-технического развития. В данном случае может оказаться весьма продуктивным декомпозиционный прием – разработка соответствующих региональных соглашений, объединяющих государства, близкие не только территориально и культурно, но и имеющие сопоставимые уровни развития. Яркий пример – позитивные результаты, достигнутые странами-участниками Европейского экономического сообщества (ЕЭС).

Первый «прорыв» в данной области – глава 5 отчета Комиссии ЕЭС по авторско-правовой охране (“Green Paper on Copyright”), представленного в 1988 г. Указанная глава была посвящена вопросам авторско-правовой охраны ЭВМ и явилась результатом анализа правовой охраны этих объектов на национальном уровне. Основным итогом данной работы был проект соответствующей директивы, принятой впоследствии Советом ЕЭС - директива Совета 91.250.ЕЭС от 14 мая 1991 г. Директива устанавливала минимальный перечень норм, которые должны быть отражены в национальном законодательстве стран-участниц в срок до начала 1993 г.

Той же Комиссией ЕЭС подготовлен проект директивы о правовой охране баз данных, принятый Советом ЕЭС в 1996 г. В большинстве Европейских стран, как и в США, и в ряде других развитых стран электронные базы данных рассматриваются как сборники – аналогично энциклопедиям, каталогам и т.п. Тем не менее, в некоторых госу-

дарствах национальное законодательство по авторско-правовой охране выделяет базы данных на электронных носителях в качестве специальных объектов охраны (характерный пример – Япония).

1.2. Отечественная история развития авторского права на программное обеспечение

В СССР проблема правовой охраны программного продукта впервые начала серьезно обсуждаться в начале 70-х годов. Однако в силу ряда факторов, в том числе в силу социально-экономической специфики нашего общества в указанный период, рассмотрение соответствующих вопросов первоначально не получило широкого внимания, ограничивалось узким кругом специалистов - сотрудников научно-исследовательских организаций. «Видимые» результаты этого периода свелись в основном к публикации материалов в рамках трудов национальной группы АИППИ.

Первым значительным актом нормотворчества на территории нашей страны в рассматриваемой сфере правового регулирования следует считать постановление Государственного комитета по науке и технике (ГКНТ) № 581 от 10 декабря 1979 г. «О повышении эффективности функционирования и использования ГосФАП». Данное постановление предписывало создание Государственного фонда алгоритмов и программ как единой системы, объединяющей многочисленные отраслевые и территориальные фонды, которые были в свое время учреждены постановлениями ГКНТ (№28 от 1966 г., № 443 от 1969 г., № 258 от 1975 г.).

В соответствии с постановлением № 581 разработчики программного продукта были обязаны в течение трех месяцев после завершения разработки провести ее испытание и сдать в систему ГосФАП программные средства, сопровожденные текстовой и эксплуатационной документацией, а также обеспечивать дальнейшее сопровождение и обновление. Фонд имел право тиражировать программные средства по запросам любых пользователей за символическую плату, сопоставимую с затратами на тиражирование. Никакое дополнительное вознаграждение авторам при таком тиражировании не предусматривалось, так как считалось, что их трудозатраты полностью компенсиро-

вались заработной платой, полученной по месту работы в период создания разработки. При такой постановке вопроса, когда в результате внедрения разработки ее авторы и их руководители имели только дополнительные обязанности, было трудно ожидать серьезной материальной заинтересованности в продвижении программного продукта как лично от авторов, так и от организаций-разработчиков.

В качестве попытки исправить ситуацию следует рассматривать принятое в феврале 1984 г. постановление ГКНТ № 41, согласованное с рядом заинтересованных министерств и ведомств. В силу данного постановления программы для ЭВМ могли быть приравнены к объектам новой техники, и, следовательно, по действующему на тот момент законодательству авторы разработок могли получать премию в размере до шести должностных окладов в год. С теоретической точки зрения постановление № 41 рассматривало ПО не как объект авторского права, а как продукцию производственно-технического назначения. Такая замена понятий была лексически отражена введением в правовую лексику нового термина «программный продукт», впервые официально употребленного в данном постановлении и включенного впоследствии в соответствующий ГОСТ 28806-90. Данный термин используется до сих пор, однако в настоящее время в связи с изменениями в законодательстве он утратил первоначальный смысл.

Существенным толчком к развитию нормативной базы охраны программных средств следует считать создание в 1987 г. Государственного комитета СССР по вычислительной технике и информатике (ГКВТИ). Одним из результатов деятельности ГКВТИ является подготовка и принятие Советом Министров СССР в апреле 1988 г. постановления № 511 «Об улучшении работ в области программного обеспечения вычислительной техники и информатики». В соответствии с этим постановлением в течение 1988 г. в СССР было разработано более двух десятков нормативных документов, в том числе «Положение об учете и охране авторских прав разработчиков программных средств вычислительной техники и информатики». Такой «мощный» пакет нормативных актов, в общем, сыграл позитивную роль в развитии правовой охраны программных продуктов в нашей стране, но в то же время обладал рядом недостатков. В частности, в указанных актах

программные средства рассматриваются одновременно как объекты авторского права и вещного права.

В 1989-1990 гг. силами СНПО «Алгоритм» при ГКВТИ была предпринята попытка преодолеть вышеуказанные недостатки и разработать новое положение о правовой охране программ для ЭВМ как объектов авторского права. Разработанный проект не успел пройти рассмотрение в Совете Министров СССР в связи с распадом СССР в 1991 г.

Подводя черту под почти 25-летней дискуссией советских юристов об основной форме охраны программных средств, отметим, что в конечном счете законодатель склонился к тому, чтобы приравнять программы для ЭВМ к произведениям литературы, науки и искусства. Такое решение было закреплено законодательно в Основах гражданского законодательства в 1991 г., где программы ЭВМ и базы данных отнесены к объектам авторского права, и в Законе СССР «Об изобретениях в СССР» 1991 г., где было установлено, что программы для ЭВМ и алгоритмы не являются изобретениями.

Впоследствии данная позиция была воспринята российским законодательством. Впервые в законодательстве новой России программы для ЭВМ и базы данных были упомянуты как объекты интеллектуальной собственности в ст. 2 Закона РСФСР «О собственности в РСФСР» от 24 декабря 1990 г. Однако данный закон ограничился декларативным отнесением программных средств к охраняемым объектам.

Правовая охрана основных программных средств впервые в полном объеме введена в Российской Федерации Законом «О правовой охране программ для электронных вычислительных машин и баз данных» 20 октября 1992 г. Принятие данного закона было предусмотрено российско-американским (советско-американским) торговым соглашением, подписанным в июне 1990 г. и ратифицированным в июне 1992 г. Данный закон, также как и принятый в 1993 г. Закон Российской Федерации «Об авторском праве и смежных правах», разработан с учетом основных положений вышеупомянутой директивы ЕЭС 1991 г. и окончательно фиксирует в российском законодательстве принадлежность программ ЭВМ и баз данных к объектам, охраняемым авторским правом.

1.3. Международно-правовые акты, регулирующие защиту авторских прав

К международным актам, участником которых является Россия и действие которых распространяется на защиту прав авторов, относятся:

- Бернская конвенция об охране литературных и художественных произведений в редакции 1971 г. (Бернский Союз);

- Всемирная конвенция по охране авторского права, разработанная по инициативе ЮНЕСКО и подписанная в 1952 г.;

- Стокгольмская конвенция от 14 июля 1967 г. об учреждении Всемирной организации интеллектуальной собственности (ВОИС).

В настоящее время Россия имеет ряд двухсторонних соглашений по вопросам защиты прав авторов, и существенным продвижением вперед в этой области стало присоединение России в 1994 г. к Бернской конвенции об охране литературных и художественных произведений и Всемирной конвенции об авторском праве.

Бернская конвенция об охране литературных и художественных произведений является старейшим актом в области охраны авторских прав и была заключена в 1886 г. В дальнейшем она неоднократно изменялась и редактировалась и на сегодня это наиболее регламентированный международный акт, обеспечивающий защиту интересов авторов (в том числе и программ для ЭВМ в странах, где по национальному законодательству они защищаются авторским правом) в иностранных государствах.

Бернская конвенция вводит ряд основных принципов охраны произведений:

- принцип ассимиляции - национальный режим охраны в стране происхождения и свой национальный режим охраны в других странах Бернского союза плюс права, «особо предоставляемые конвенцией»;

- национальный принцип - предоставление охраны вне зависимости от места первой публикации, основываясь на гражданстве или постоянном проживании автора в стране-участнице;

- территориальный принцип - предоставление охраны вне зависимости от гражданства или постоянного пребывания в странах-участниках, основываясь на месте первой (или одновременной) публикации в одной из стран Бернского союза;

- принцип автоматической охраны, согласно которому предоставляемая охрана не должна обусловливаться соблюдением каких-либо формальностей;

- минимальный обязательный (50-летний) срок охраны авторского права, исчисляемый со дня смерти автора.

В соответствии со статьей 5 в отношении произведений, по которым авторам предоставляется охрана в силу настоящей Конвенции, авторы пользуются в странах Союза, кроме страны происхождения произведения, правами, которые предоставляются в настоящее время или будут предоставлены в дальнейшем соответствующими законами этих стран своим гражданам, а также правами, особо предоставляемыми настоящей Конвенцией. Охрана в стране происхождения регулируется внутренним законодательством. Однако, если автор не является гражданином страны происхождения произведения, в отношении которого ему предоставляется охрана в силу настоящей Конвенции, он пользуется в этой стране такими же правами, как и авторы - граждане этой страны. Наряду с гражданством важную роль играет и страна первого опубликования произведения (страна происхождения). Опубликованные впервые в стране члене Союза или одновременно в нескольких странах, одна из которых является членом Союза, произведения подлежат защите на основании данной Конвенции. Произведение считается опубликованным одновременно, если его публикация в другой стране имела место в течение 30 дней после первого опубликования.

Под принципом минимальности права понимается обязанность государства-участника обеспечить минимум правовой охраны иностранным произведениям и определить минимальный уровень охраны авторских прав в странах-участниках Союза.

Всемирная конвенция об авторском праве была подписана в Париже в 1952 г. (к этой редакции Россия присоединилась в 1973 г.) и была пересмотрена одновременно с Бернской конвенцией в 1971 г. (к этой редакции Россия присоединилась только в 1995 г.). Всемирная конвенция строится на принципе национального режима с менее жесткими правовыми рамками для стран-участников и имеет дополнительный раздел "Специальные положения, относящиеся к развивающимся странам", устанавливающий ряд льгот для развивающихся стран.

В данном разделе определяется, что если присоединившаяся к Конвенции развивающаяся страна, учитывая свое экономическое положение и свои социальные и культурные потребности, не считает себя в состоянии немедленно ввести в действие положение по охране всех прав, предусмотренных настоящим актом, то при соблюдении ряда правил она пользуется льготами, установленными Конвенцией. Это положение создает предпосылки для установления адекватного режима защиты авторских прав в развивающихся странах.

Для обеспечения более эффективной защиты прав авторов и правообладателей в этой сфере 14 июля 1967 г. была заключена *Стокгольмская конвенция* об учреждении всемирной организации интеллектуальной собственности (ВОИС). В соответствии со ст. 2 Конвенции, интеллектуальная собственность включает права, относящиеся:

- к литературным, художественным и научным произведениям; исполнительской деятельности артистов, звукозаписи, радио- и телевизионным передачам;

- изобретениям во всех областях человеческой деятельности, научным открытиям;

- промышленным образцам;

- товарным знакам, знакам обслуживания, фирменным наименованиям, коммерческим обозначениям.

Защита против недобросовестной конкуренции, а также все другие права, относящиеся к интеллектуальной деятельности в производственной, научной, литературной и художественной областях.

Всемирная организация интеллектуальной собственности (ВОИС), которая является учреждением ООН, ответственным за функционирование международной системы защиты интеллектуальной собственности, и разрабатывает соответствующие правовые вопросы, относит к интеллектуальной собственности информацию, которая может быть представлена на материальном носителе и распространена на неограниченном количестве копий.

1.4. Современное положение авторских прав на рынке программного обеспечения в России

На современном этапе развития авторского права на ПО производители сталкиваются с таким явлением, как «компьютерное пиратство».

Сегодня тема компьютерного пиратства занимает чуть ли не второе место после политики. В то же время однозначного определения этого явления нет - различные группы трактуют его по-разному. Если проанализировать определения «компьютерного пиратства», предоставляемые Microsoft и BSA, то любой легальный пользователь, сделавший «шаг в сторону» от строгого соблюдения требований лицензионного соглашения, автоматически попадает в категорию «пиратов». Учитывая, что лицензионные соглашения нередко запрещают то, что по закону запретить нельзя (например исследование двоичного кода продукта), и требуют того, что противоречит социальным традициям (например не делиться музыкой и программами с родственниками и друзьями), подобные определения едва ли можно считать адекватными, в противном случае «пиратство» победить принципиально невозможно, так как для этого требуется «сломать» устои современного общества. Кроме того, такие определения находятся и в противоречии с практикой. Под «пиратством», хотя и не в явной форме, все же понимается определенная организованная деятельность, направленная на получение дохода за счет нарушения авторских прав.

Компьютерное пиратство, по сути, является воровством программного продукта путем незаконного копирования подлинных программ, распространения неавторизованных версий программного обеспечения либо подделки программного обеспечения и распространения программ-имитаций. Компьютерное пиратство также имеет место, когда кто-либо производит большее количество копий легально приобретенного продукта, чем предусмотрено условиями лицензии, либо одалживает свою копию программы другому лицу.

Нарушения авторских прав в области программного обеспечения относятся к компьютерным преступлениям. Компьютерные преступления совершаются во всем мире.

Основная причина - экономическая. Программный продукт является товаром, который имеет автора, цену, гарантии качества. Этот товар можно купить, продать, обменять и т.п. И как любой товар он может быть объектом кражи и незаконного использования. Подделкой программного обеспечения занимаются много людей, так как это очень выгодный бизнес.

Кроме экономических причин, на рост нелегального использования программных продуктов влияет и раннее обучение работе на компьютере детей. С целью ознакомления с работой программ подростки копируют буквально все попадающиеся им программы, оставляя себе наиболее понравившиеся продукты. Наличие свободного времени, желание просто разобраться в программе, а нередко и желание похвастаться перед товарищами своими способностями заставляют их заниматься вскрытием программных защит. Затем, не думая о возможных последствиях, они учат этому друг друга. Как правило, подростки и не подозревают, что нарушают тем самым закон.

1.5. Контрольные вопросы, задания, темы рефератов

А. Контрольные вопросы

1. Каковы основные точки зрения на возможности правовой защиты программных средств как специфического объекта интеллектуальной собственности?
2. На основании чего законодатель склонился к тому, чтобы приравнять программы ЭВМ к произведениям литературы, науки и искусства. Какие правовые последствия имело это решение?
3. Когда возникла проблема «компьютерного права»?
4. В каком году впервые была зарегистрирована программа ЭВМ в качестве объекта правовой охраны?
5. Определения каких понятий были рассмотрены в Типовых положениях по охране программного обеспечения вычислительных машин, принятых ВОИС в 1978 г.?
6. Что предписывало постановление Государственного комитета по науке и технике (ГКНТ) № 581 от 10 декабря 1979 г. «О повышении эффективности функционирования и использования ГосФАП»?
7. Чем являлось ПО с точки зрения постановления ГКНТ № 41?
8. Участником каких международных актов по защите авторских прав является Россия?

9. Какие права включает в себя «интеллектуальная собственность»?
10. Что такое «компьютерное пиратство»?

Б. Задания

1. Проанализируйте последствия принятия поправок к национальным законодательствам об авторских правах в начале 80-х годов.
2. Поясните содержание и значение главы № 5 отчета Комиссии ЕЭС по авторско-правовой охране (“Green Paper on Copyright”), представленного в 1988 г.
3. Дайте общую характеристику основным международным организациям и правовым документам по защите авторских прав.
4. Проанализируйте этапы развития юридической защиты программного обеспечения (программного продукта).
5. Проанализируйте последствия деятельности «компьютерных пиратов» на конкретном примере.

В. Темы рефератов

1. Причины возникновения проблемы «компьютерного права».
2. Деятельность Государственного фонда алгоритмов и программ и Государственного комитета СССР по вычислительной технике и информатике.
3. Анализ прецедентов судебных разбирательств по защите авторских прав на программное обеспечение на территории РФ, США, Англии, Франции и Японии.
4. Нормы Всемирной (Женевской) конвенции по охране прав авторов программ.
5. Нормы Бернской конвенции об охране литературных и художественных произведений.
6. Стокгольмская конвенция об учреждении всемирной организации интеллектуальной собственности (ВОИС).
7. Причины возникновения и развития «компьютерного пиратства».
8. Последствия деятельности «компьютерных пиратов».

Глава 2. ПРАВОВОЙ ИНСТИТУТ АВТОРСКОГО ПРАВА КАК ОСНОВА ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Введение

Отрасль информационных технологий интенсивно развивается. То программирование, о котором говорили как о форме творчества, уходит на второй план и на смену ему приходит программирование коммерческое. Растущие мощности компьютеров позволяют составителям программ не очень заботиться об их скорости и компактности, что ведет к реализации алгоритмов напрямую, без внесения творческого вклада собственно в процесс программирования. Средства визуального программирования (например Visual Basic) позволяют превратить процесс написания программы в применение примитивного набора стандартных приемов. Нельзя назвать творческим процессом действия, которые могут быть повторены любым специалистом и приведут к идентичным результатам. Такой процесс называется ремеслом.

Однако отсюда не стоит делать выводов о том, что программы - как результат ремесла - не требуют защиты в рамках института исключительных прав. Исключительные права вытекают не из творческого характера или изобретательского уровня программы, а из ее нематериальной природы. Такое право не является чем-то принципиально новым, а лишь естественным образом применяет устоявшиеся правовые принципы к объектам с другими натуральными свойствами. Однако целесообразность наличия личных неимущественных прав создателя программы в этом свете вызывает сомнение. Но как же быть? Ведь, несомненно, последовательность операторов, как и любой другой объект интеллектуальной деятельности, требует защиты. В первую очередь защиты от распространения третьими лицами. Эта защита нужна программам в силу того, что затраты на их производство несравнимы с затратами на их тиражирование. Ведь защищая программу, мы защищаем вложенные в нее инвестиции.

В главе рассматриваются наиболее существенные для разработчиков программных продуктов положения законодательства РФ об

авторском праве, применяемом к компьютерным программам. А также проанализированы некоторые недостатки законодательной базы, очевидность которых была продемонстрирована правоприменительной практикой.

2.1. Законы по защите авторских прав

Авторские права охраняются специальными законами как на национальном, так и на международном уровнях.

Законодательство Российской Федерации об авторском праве состоит из положений:

- Конституции Российской Федерации, принятой 12 декабря 1993 г. (ст. 44, п.1);
- Гражданского кодекса Российской Федерации (ч.4, разд. 7);
- Закона РФ № 5352-1 от 9 июля 1993 г. (с последующими изменениями) «Об авторском праве и смежных правах»;
- Закона РФ № 3523-1 от 23 сентября 1992 г. «О правовой охране программ для электронно-вычислительных машин и баз данных»;
- Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
- Указа Президента РФ от 5 декабря 1998 г. № 1471 «О мерах по реализации прав авторов произведений, исполнителей и производителей фонограмм на вознаграждение за воспроизведение в личных целях аудиовизуального произведения или звукозаписи произведения»;
- Указа Президента РФ от 7 октября 1993 г. № 1607 «О государственной политике в области охраны авторского права и смежных прав»;
- Бернской конвенции по охране литературных и художественных произведений от 9 сентября 1886 г;
- Всемирной конвенции об авторском праве от 6 сентября 1952 г. (пересмотрена в Париже 24 июля 1971 г.);
- Договора ВОИС по авторскому праву (WCT) (принят Дипломатической конференцией в Женеве 20 декабря 1996 г.).

Рассмотрим наиболее существенные для разработчиков программных продуктов положения законодательства об авторском праве, применяемом к компьютерным программам.

2.2. Основные положения законодательства об авторском праве на территории Российской Федерации

Программы для ЭВМ Гражданским кодексом Российской Федерации относятся к объектам авторских прав. Программа для ЭВМ определяется в Законе как «… объективная форма представления совокупности данных и команд, предназначенных для функционирования электронных вычислительных машин (ЭВМ) и других компьютерных устройств с целью получения определенного результата. Под программой для ЭВМ подразумеваются также подготовительные материалы, полученные в ходе ее разработки, и порождаемые ею аудиовизуальные отображения».

Охрана программ для ЭВМ распространяется на все виды программ для ЭВМ (в том числе на операционные системы), которые могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код».

Авторское право на программу для ЭВМ возникает в силу факта ее создания. Для признания и осуществления авторского права на программу для ЭВМ или базу данных не требуется депонирования, регистрации или соблюдения иных формальностей.

Здесь разработчикам следует обратить внимание на то, что для признания и осуществления авторского права на компьютерную программу закон не требует обязательной регистрации программ.

Учитывая, что правовая охрана программ для ЭВМ и баз данных возникает с момента создания, а их регистрация носит факультативный характер, возникает вопрос о целесообразности их регистрации. Такая регистрация имеет ряд преимуществ:

- происходит оповещение специалистов о создании новой программы для ЭВМ или базы данных и о наличии на них прав у правообладателя;

- имеет место дополнительная реклама, поскольку происходит публикация в бюллетене РосАПО;

- при возникновении конфликтных ситуаций существенно увеличиваются правовые возможности правообладателя, поскольку депонируемые в РосАПО материалы могут рассматриваться судом в качестве доказательства наличия соответствующих прав у лица, подавшего заявку.

Автором компьютерной программы признается физическое лицо, творческим трудом которого она создана.

Право авторства, право на имя и право на защиту репутации автора охраняются бессрочно. Имущественные права действуют в течение всей жизни автора и 70 лет после его смерти. В отношении анонимного произведения или произведения под псевдонимом срок охраны составляет 70 лет с момента первого правомерного опубликования произведения.

Разработчикам программ следует учитывать, что предоставляемая охрана не распространяется на идеи и принципы, лежащие в основе компьютерной программы. В том числе эта охрана не распространяется на методы функционирования программы. Следовательно, охраняется законом не идея, заложенная в алгоритм, а лишь конкретная реализация этого алгоритма в виде последовательности операторов и действий над этими операторами.

Таким образом, защищать разработчику необходимо прежде всего эту конкретную форму - исходный текст и/или объектный код программы.

Для оповещения о своих исключительных имущественных правах их обладатель вправе использовать знак охраны авторского права, который помещается на каждом экземпляре произведения и обязательно состоит из трех элементов:

- латинской буквы "С" в окружности - ©;

- имени (наименования) обладателя исключительных имущественных прав;

- года первого опубликования произведения.

Специфической чертой авторского права считается его строго территориальный характер, т.е. сфера действия права на программу определяется территорией государства, где это право возникло, и ограничивается пределами этого государства. В другом государстве при отсутствии международного соглашения это право не признается. Для того чтобы компьютерные программы обеспечивались защитой в других государствах, необходимо, чтобы эти государства либо заключили между собой соглашения о взаимном признании и защите авторских прав, либо являлись участниками международных актов об авторском праве.

2.3. Права разработчиков программного обеспечения

Права авторов компьютерных программ подразделяются на личные неимущественные и имущественные права.

Необходимо подчеркнуть, что личные права принадлежат автору независимо от его имущественных прав.

Обратим внимание на личные права, принадлежащие автору программы:

- право авторства, то есть право признаваться автором произведения. Разработчикам программ в связи с этим следует иметь в виду, что при отсутствии доказательств иного автором произведения считается лицо, указанное в качестве автора на оригинале или экземпляре произведения (презумпция авторского права). А если возникают сомнения в авторстве какого-либо лица в отношении определенной компьютерной программы, то эти сомнения могут быть разрешены только судом;

- право на имя, то есть «право использовать или разрешать использовать произведение под подлинным именем автора, псевдонимом или без обозначения имени, то есть анонимно». Заметим, что если программа для ЭВМ не имеет указания на имя автора, организация, наименование которой обозначено на программном продукте при отсутствии доказательств иного, считается представителем автора и в этом качестве имеет право защищать права автора, а также обеспечивать их осуществление;

- право на неприкосновенность, то есть «право на защиту произведения, включая его название, от всякого искажения или иного посягательства, способного нанести ущерб чести и достоинству автора». Это право в отношении компьютерных программ предусматривает, что для этих произведений наибольшее значение имеет внесение в них без ведома автора таких изменений и уточнений, которые могут отразиться на функциональных свойствах и характеристиках. Ущерб чести и достоинству автора программы может быть следствием несанкционированного вмешательства других лиц. То есть никто не может использовать программу и не может вносить в нее изменения без согласия автора;

- право на обнародование, то есть право обнародовать или разрешать обнародовать произведение в любой форме. Имущественные права автора компьютерной программы сводятся к исключительному праву осуществлять или разрешать осуществление ряда действий;

- воспроизведение, то есть изготовление одного или более экземпляров произведения в любой материальной форме, включая постоянное или временное хранение в цифровой форме в электронном средстве;

- распространение оригинала или экземпляров произведения посредством продажи или иной передачи права собственности;

- прокат оригиналов или экземпляров компьютерных программ независимо от принадлежности права собственности на оригинал или экземпляры произведений. Заметим, что данное право не применяется в отношении компьютерных программ, если сама программа не является основным объектом проката;

- перевод произведения на другой язык;

- переделку или иную переработку программы и другие.

2.4. Защита личных и исключительных прав

За защитой своих нарушенных прав автор компьютерной программы может обратиться в судебные или другие органы в соответствии с их компетенцией. При этом он может предъявить требования:

А. При нарушении личных (неимущественных прав):

- признания авторского права;

- восстановления положения, существовавшего до нарушения авторского права;

- пресечения действий, нарушающих авторские права или создающих угрозу их нарушения;

- компенсацию морального вреда;

- публикации решения суда о допущенном нарушении.

Б. При нарушении исключительных прав (имущественных):

- о признании права - к лицу, которое отрицает или иным образом не признает право, нарушая тем самым интересы правообладателя;

- о пресечении действий, нарушающих право или создающих угрозу его нарушения, - к лицу, совершающему такие действия или осуществляющему необходимые приготовления к ним;

- о возмещении убытков - к лицу, неправомерно использовавшему результат интеллектуальной деятельности или средство индивидуализации без заключения соглашения с правообладателем (бездоговорное использование) либо иным образом нарушившему его исключительное право и причинившему ему ущерб;

- об изъятии материального носителя и уничтожению за счет нарушителя, если законом не предусмотрено их обращение в доход Российской Федерации;

- о публикации решения суда о допущенном нарушении с указанием действительного правообладателя - к нарушителю исключительного права.

Правообладатель может требовать от нарушителя:

- по выбору либо возмещения убытков, включая упущенную выгоду, либо взыскания дохода, полученного нарушителем вследствие нарушения авторского права, либо выплаты компенсации в размере от 10 тысяч рублей до 5 миллионов рублей, определяемым по усмотрению суда, арбитражного суда или третейского суда исходя из характера нарушения;

- выплаты компенсации за каждый случай неправомерного использования произведений или объектов смежных прав либо за допущенные правонарушения в целом - в двукратном размере стоимости экземпляров произведений или объектов смежных прав либо в двукратном размере стоимости прав на использование произведений или объектов смежных прав, определяемой исходя из цены, которая при сравнимых обстоятельствах обычно взимается за правомерное использование произведений или объектов смежных прав.

Компенсация подлежит взысканию при доказанности факта правонарушения независимо от наличия или отсутствия убытков.

Весьма серьезная ответственность установлена за нарушение авторских прав и Уголовным кодексом Российской Федерации. Так, в соответствии со ст. 146 УК РФ (Нарушение авторских и смежных прав) «незаконное использование объектов авторского права или смежных прав, а равно присвоение авторства, если эти деяния причинили крупный ущерб… наказываются штрафом в размере от двухсот до четырехсот минимальных размеров оплаты труда или в размере заработ-

ной платы или иного дохода осужденного за период от двух до четырех месяцев, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо лишением свободы на срок до двух лет». И далее: «… те же деяния, совершенные неоднократно либо группой лиц по предварительному сговору или организованной группой, наказываются штрафом в размере от четырехсот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от четырех до восьми месяцев, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до пяти лет».

Как видно, уголовная ответственность наступает при наличии «крупного ущерба», его критериями являются размер причиненного ущерба, количество потерпевших, степень нарушения прав гражданина, тяжесть причиненного морального вреда. В судебной практике крупным ущербом признается ущерб, превышающий десятикратный минимальный размер оплаты труда.

2.5. Свободное воспроизведение и адаптация программы для ЭВМ или базы данных

В нормах российского авторского права действия, которые можно и нельзя осуществлять без согласия автора, содержатся в ст. 15 Закона «О правовой охране программ для ЭВМ и баз данных». Приведем наиболее существенные выдержки из нее:

«…Лицо, правомерно владеющее экземпляром программы для ЭВМ или базы данных, вправе без получения дополнительного разрешения правообладателя осуществлять любые действия, связанные с функционированием программы для ЭВМ или базы данных в соответствии с ее назначением, в том числе запись и хранение в памяти ЭВМ, а также исправление явных ошибок. Запись и хранение в памяти ЭВМ допускаются в отношении одной ЭВМ или одного пользователя в сети, если иное не предусмотрено договором с правообладателем».

«… Лицо, правомерно владеющее экземпляром программы для ЭВМ, вправе без согласия правообладателя и без выплаты дополнительного вознаграждения декомпилировать или поручать декомпили-

рование программы для ЭВМ с тем, чтобы изучать кодирование и структуру этой программы при следующих условиях:

- информация, необходимая для взаимодействия независимо разработанной данным лицом программы для ЭВМ с другими программами, недоступна из других источников;

- информация, полученная в результате этого декомпилирования, может использоваться лишь для организации взаимодействия независимо разработанной данным лицом программы для ЭВМ с другими программами, а не для составления новой программы для ЭВМ, по своему виду существенно схожей с декомпилируемой программой для ЭВМ или для осуществления любого другого действия, нарушающего авторское право.

Декомпилирование осуществляется в отношении только тех частей программы для ЭВМ, которые необходимы для организации такого взаимодействия».

Действия, которые можно или нельзя осуществлять без автора, разграничиваются с помощью понятий адаптации, модификации и декомпилирования программы для ЭВМ.

Адаптация программы для ЭВМ или базы данных - это внесение изменений, осуществляемых исключительно в целях обеспечения функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя.

Адаптация может осуществляться законным пользователем экземпляра программы без согласия правообладателя и без выплаты ему дополнительного вознаграждения.

Модификация (переработка) *программы* для ЭВМ или базы данных - это любые их изменения, не являющиеся адаптацией.

Перевод программы для ЭВМ – частный случай модификации. Для осуществления модификации требуется согласие правообладателя. При этом исправление явных ошибок не относится к модификации, поэтому это действие может осуществляться законным пользователем экземпляра программы также без согласия правообладателя и без выплаты дополнительного вознаграждения.

Необходимо обратить внимание на относительную условность границы между адаптацией и модификацией компьютерной программы. Если какое-либо лицо произвело изменения в программе для своего личного компьютера в режиме конечного пользователя, то это действие может рассматриваться как адаптация данной программы. Но если это же лицо в дальнейшем начнет распространение измененной таким образом программы для других пользователей данного класса ЭВМ, то это действие будет рассматриваться как модификация. При этом дальнейшее распространение модифицированной программы потребует специального разрешения ее законного правообладателя.

Декомпилирование программы для ЭВМ - это технический прием, включающий преобразование объектного кода в исходный текст в целях изучения структуры и кодирования программы для ЭВМ.

Законный пользователь может осуществлять декомпилирование или поручать другим лицам выполнять это действие без согласия правообладателя и без выплаты дополнительного вознаграждения, если полученная в результате информация необходима для организации взаимодействия независимо созданной этим лицом программы с другими программами и является недоступной из других источников. При этом не допускается использовать полученную в результате декомпилирования информацию для составления новой программы, по своему виду существенно схожей с декомпилируемой, или для осуществления любого другого действия, нарушающего авторское право.

2.6. Положения законодательства о соавторстве и об авторском праве на служебные произведения

На практике программное обеспечение часто создается коллективом разработчиков. Если программа создана в результате совместной творческой деятельности двух или более лиц, то «… граждане, создавшие произведение совместным творческим трудом, признаются соавторами независимо от того, образует ли такое произведение неразрывное целое или состоит из частей, каждая из которых имеет самостоятельное значение».

Основанием для соавторства является совместный творческий труд в решении поставленной задачи. При этом не важно, какова доля участия каждого из соавторов, важен сам факт такого участия. Право на использование произведения в целом принадлежит соавторам совместно. Каждый из соавторов вправе использовать созданную им часть произведения, имеющую самостоятельное значение (если она может быть использована независимо от других частей этого произведения), по своему усмотрению, если иное не предусмотрено соглашением между ними.

Большинство компьютерных программ создается как выполнение служебного задания нанимателя. Поэтому разработчикам программного обеспечения необходимо знать положения законодательства об авторском праве, регулирующие отношения между автором и работодателем в части служебных произведений.

Имущественные права на созданное в порядке выполнения служебного задания или по прямому указанию работодателя произведение принадлежат нанимателю, если в договоре между ним и автором не предусмотрено иное.

А вот личные неимущественные права на произведение, созданное в порядке выполнения служебного задания или служебных обязанностей (служебное произведение), принадлежат автору.

Необходимо отметить, что если работодатель не желает заключать договор с автором, то исключительные имущественные права на использование принадлежат работодателю.

Следовательно, при отсутствии соответствующего договора или надлежащей записи в договоре с автором работодатель (по умолчанию) является владельцем исключительных имущественных прав на служебные произведения, созданные лицами, находящимися с ним в трудовых отношениях.

Обладание исключительными имущественными правами на произведение накладывает на работодателя по отношению к авторам определенные обязанности. При наличии договора между ними автор может претендовать на вознаграждение как за создание, так и за каждый вид использования произведения. Порядок выплаты и размер вознаграждения устанавливаются договором между работником и работодателем.

2.7. Регистрация компьютерных программ

Разработчик может заранее предпринять определенные предварительные действия по защите своих авторских прав. Предварительными действиями по защите авторских прав может служить регистрация программ.

Регистрация авторских прав на определенное произведение ставит автора этого произведения в привилегированное положение по отношению к авторам незарегистрированных работ. Хотя нормы российского авторского права (в отличие от норм американского авторского права) не требуют обязательной регистрации программных продуктов, такая регистрация в большинстве случаев существенно упростила и облегчила бы подтверждение факта авторства при наличии спора между потенциальными авторами компьютерной программы.

Система регистрации объектов интеллектуальной собственности дает ряд преимуществ.

Во-первых, посредством регистрации устанавливается презумпция того, что работа защищена авторским правом и что все третьи лица предупреждены об ответственности за незаконное (несанкционированное автором) пользование данным объектом интеллектуальной собственности. Польза от этого в том, что потенциальный ответчик (нарушитель авторских прав) не сможет в суде оспорить само существование авторских прав истца.

Во-вторых, регистрация содействует защите прав в случаях возникновения конфликтных ситуаций. Депонированные материалы рассматриваются судом в качестве первоочередного свидетельства наличия соответствующих прав.

Регистрация делает возможным предъявление требования к ответчику о возмещении расходов, связанных с оплатой адвокатских услуг, которые обычно составляют значительную часть от всего ущерба, причиненного нарушением. Возможность получить возмещение своих затрат на услуги адвоката в связи с судебным разбирательством является чрезвычайно важной льготой.

На практике при судебном рассмотрении дел в России серьезным аргументом признается предоставление свидетельства о регист-

рации программы, выданного Российским агентством по правовой охране программ для ЭВМ и баз данных и топологий интегральных микросхем (РосАПО). Одной из важных обязанностей РосАПО считается регистрация программ для ЭВМ и баз данных, а также публикация сведений о зарегистрированных объектах (в официальном бюллетене РосАПО). На зарегистрированные программы Агентство выдает свидетельства, которые носят правоудостоверяющий характер. Свидетельства выдаются под ответственность заявителя, экспертиза объекта по существу не производится. Поэтому свидетельство удостоверяет, что на указанную в нем дату указанные в нем правообладатель(ли) и (или) авторы зарегистрировали на свое имя программу для ЭВМ или базу данных, а объем прав подтверждается приложенной к заявлению об официальной регистрации надлежащим образом заверенной распечаткой исходного текста программы.

В Российской Федерации появились также коммерческие организации по оказанию услуг правообладателям и авторам при регистрации ими в РосАПО программ для ЭВМ или баз данных. Такие услуги оказывают как объединения патентных поверенных, так и региональные и специализированные центры правовой охраны, аккредитованные при РосАПО.

Первым шагом на пути к приобретению авторских прав на программы для ЭВМ и баз данных является подача заявки на регистрацию в федеральную службу Роспатент.

Правильно оформленная заявка принимается к рассмотрению федеральным органом исполнительной власти по интеллектуальной собственности. Если по итогам рассмотрения заявки принято решение о предоставлении регистрации указанной в поданном документе программы для ЭВМ или базы данных, то программа для ЭВМ или база данных вносится в реестр программ для ЭВМ или реестр баз данных, правообладателю направляется уведомление об официальной регистрации и выдается свидетельство об официальной регистрации.

Федеральный орган исполнительной власти по интеллектуальной собственности публикует сведения об официальной регистрации программы для ЭВМ или базы данных в своем официальном бюллетене.

2.8. Контрольные вопросы, задания, темы рефератов

А. Контрольные вопросы

1. Каковы неимущественные права авторов программного обеспечения?
2. Каковы имущественные права авторов программного обеспечения?
3. В силу чего возникло авторское право на программу для ЭВМ?
4. Как в законе определяется «программа для ЭВМ»?
5. Обязательна ли по закону регистрация программного продукта?
6. В течение какого времени действуют имущественные права автора?
7. Что представляет собой знак охраны авторского права?
8. В чем заключается строго территориальный характер защиты авторского права?
9. Что такое «право на имя»?
10. Какие требования может предъявить автор программного обеспечения при обращении в суд из-за нарушения своих прав?

Б. Задания

1. Сформулируйте основные права разработчика программного обеспечения.
2. Рассмотрите виды уголовной ответственности за нарушение авторских прав на программное обеспечение.
3. Создайте пакет документов для подачи прошения о заведении уголовного дела по нарушению авторских прав на программное обеспечение.
4. Проследите изменения положения авторского права на служебное произведение.
5. Перечислите преимущества регистрации программного обеспечения.
6. Приведите и раскройте основные положения законодательства об авторском праве на территории Российской Федерации.

В. Темы рефератов

1. Анализ и сравнение законодательных баз по защите авторских прав на программное обеспечение РФ и США.
2. Анализ и сравнение законодательных баз по защите авторских прав на программное обеспечение РФ и Франции.
3. Воспроизведение и адаптация программы для ЭВМ или базы данных с юридической точки зрения.
4. Положения законодательства о соавторстве. Судебная практика.
5. Положения законодательства об авторском праве на служебные произведения. Анализ ранних и современных законодательных актов.
6. Правила и формы регистрации компьютерных программ на территории РФ.
7. Правила и формы регистрации компьютерных программ на территории США.

Глава 3. ТЕХНИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ АВТОРСКИХ ПРАВ НА ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Введение

При создании программного обеспечения разработчик вправе позаботиться о соблюдении своих авторских прав путем применения различных технических методов и средств. В настоящее время существует достаточно обширный арсенал программных и аппаратно-программных средств, позволяющих в той или иной степени «обезопасить» создаваемое программное обеспечение. Все они различаются эффективностью и стоимостью.

В главе рассматриваются отдельные технические методы и механизмы защиты авторского права на программное обеспечение.

3.1. Программная защита

Методы программной защиты реализуют подходы к защите авторских прав, основанные на противодействии созданию копий про-

граммы (воспроизведению) либо попыткам запуска и/или исполнения незаконной копии.

Преимуществами обладает программная защита такой сложности, при которой нарушитель для взлома защиты должен затратить средства (материальные и временные), не сравнимые со средствами, необходимыми на покупку программного продукта или создание собственного кода. Говоря другими словами, надежной является такая программная защита, если для взлома или обхода механизма защиты нарушителю необходимо обладать высоким потенциалом нападения, то есть обладать высокой квалификацией, располагать значительными материальными, трудовыми и временными ресурсами.

Следовательно, максимально возможное затруднение обнаружения, исследования и/или модификации механизма защиты - первоочередная задача автора программной защиты.

К базовым методам защиты программ от незаконного копирования отнесем:

- парольную защиту;
- шифрование;
- группу методов, предназначенных для защиты условно-бесплатных программных продуктов.

Парольная защита. Самая распространенная защита программного обеспечения. При реализации парольной защиты запуск приложения сопровождается запросом пароля и последующим сравнением введенного пароля с оригиналом.

Сразу заметим, что парольная защита может быть рекомендована только для использования при защите специализированного программного обеспечения, предназначенного для узкого круга пользователей. При широком использовании программ, защищенных таким образом, очень велика вероятность того, что хотя бы один законный пользователь сообщит пароль злоумышленнику, этого будет достаточно для того, чтобы сделать защищенное приложение общедоступным.

Хорошая система защиты организована таким образом, что, во-первых, не позволяет пользователю бесконечно вводить неправильный пароль, а ограничивает число попыток. Во-вторых, между

двумя неудачными попытками ввода пароля специально вводится временная задержка с целью уменьшить количество попыток взлома системы защиты за некоторый промежуток времени.

Даже начинающим программистам известно, что нельзя хранить пароль в открытом виде, так как, например, в случае хранения пароля непосредственно в защищаемой программе злоумышленник может легко найти эталонный пароль либо просмотрев дамп файла, в котором хранится программа, либо даже с помощью специальной программы, распечатывающей все текстовые строки.

В основном авторы защит либо шифруют пароль известными или собственными криптографическими методами, либо применяют хеш-функции (хеш-суммы) для преобразования пароля.

Метод хеширования пароля заключается в хранении в качестве эталона не собственно пароля, а результата определенных автором защиты математических преобразований (именно эти преобразования и называются хеш-функцией или хешированием) над символами пароля. При запуске приложения введенный пользователем пароль подвергается хешированию и сравнению полученного результата с эталоном.

Шифрование. Хорошо зарекомендовал себя метод шифрования пароля. Шифровка даже при использовании некриптостойких алгоритмов и коротких паролей все же требует трудоемкого изучения алгоритма, написания атакующих программ и часто очень длительного времени на поиск подходящего пароля.

Шифрование - это обратимое преобразование информации с целью сокрытия ее содержания для неавторизованных лиц. Авторизованное (неавторизованное) лицо - пользователь, имеющий (не имеющий) право на доступ к информации. Дешифрование - преобразование информации, обратное шифрованию. Методы, алгоритмы и средства шифрования информации изучает криптография. Системы, использующие шифрование информации, называют криптографическими системами, или криптосистемами.

Многие специалисты считают, что шифрование является одним из самых надежных средств безопасности данных вообще и, в частности, защиты программного обеспечения. Шифрование используется

для защиты программного обеспечения от нелегального использования, модификации, а также от исследования логики работы защищенной программы.

Подчеркнем, что для шифрования автором защиты может быть использован собственный криптоалгоритм. Но, как правило, предлагаемые алгоритмы шифрования являются слабыми, так как авторы субъективно переоценивают стойкость (надежность) собственных алгоритмов. И прежде всего потому, что далеко не все авторы защит являются специалистами в области криптоанализа.

Криптоанализ объединяет методы, алгоритмы, средства дешифрования, а также оценку стойкости криптосистем. Здесь под стойкостью (надежностью) криптоалгоритма понимают количество компьютерных операций, необходимых криптоаналитику для вскрытия ключа (или исходного текста).

Очевидно, что необходимо, чтобы число операций было настолько велико, что при реализации криптоатаки на современной вычислительной технике потребовалось бы машинное время, в течение которого зашифрованная информация потеряла бы свою ценность.

Специалисты по защите информации рекомендуют использовать известные, стойкие, математически обоснованные криптоалгоритмы с хорошо изученными свойствами и недостатками.

На практике применяются в основном два вида криптосистем:

- симметричные;
- асимметричные.

В *симметричной криптосистеме* отправитель и получатель сообщения используют один и тот же секретный ключ. Симметричная криптосистема генерирует общий секретный ключ, распределяет его между законными пользователями. С помощью этого ключа производится как шифрование, так и дешифрование сообщения. Этот ключ должен быть известен всем пользователям и требует периодического обновления одновременно у отправителя и получателя.

Процесс распределения секретных ключей между абонентами обмена конфиденциальной информации в симметричных криптосистемах имеет весьма сложный характер. Имеется в виду, что передача секретного ключа нелегитимному пользователю может привести к вскрытию всей передаваемой информации.

Наиболее известные симметричные криптосистемы - шифр Цезаря, шифр Вижинера, американский стандарт шифрования DES, шифр IDEA и отечественный стандарт шифрования данных ГОСТ 28147-89.

Асимметричные криптосистемы предполагают использование двух ключей - открытого и секретного. Первый, открытый, доступен любому пользователю, с помощью которого зашифровывается сообщение. Второй, секретный, должен быть известен только получателю сообщений.

Расшифрование сообщения с помощью открытого ключа невозможно. Для расшифрования данных получатель зашифрованного сообщения применяет второй ключ, секретный. Ключ расшифрования не может быть определен из ключа зашифрования. Схему асимметрической криптографии в 1976 г. предложили два молодых американских математика Диффи и Хеллман. Наиболее известные асимметричные криптосистемы – это шифр RSA и шифр Эль Гамаля. Данная схема является довольно-таки сложной для криптоанализа. Чем больше ключ, тем сложнее его подобрать обычным простым перебором. Для вскрытия современной криптосистемы со средней длиной ключа потребуется около 1050 машинных операций, что практически невозможно на современных компьютерных системах.

Безопасность любого криптографического алгоритма определяется используемым криптографическим ключом. Для получения ключей используются аппаратные и программные средства генерации случайных значений ключей. Как правило, применяют датчики псевдослучайных чисел. Однако степень случайности генерации чисел должна быть достаточно высокой. Идеальными генераторами являются устройства на основе натуральных случайных процессов, например на основе белого шума.

Важной задачей при работе с ключами является их распределение. В настоящее время известны два основных способа распределения ключей: с участием центра распределения ключей и прямой обмен ключами между пользователями.

На основе шифрования на практике используются следующие механизмы защиты программ:

- шифрование кода программы. Код программы шифруется с тем, чтобы быть расшифрованным только во время выполнения программы;

- шифрование фрагмента (участка) программы. Для шифрования чаще выбирается критический участок программы.

В обоих случаях может применяться как статическое, так и динамическое шифрование. При статическом шифровании весь код (фрагмент кода) один раз шифруется/дешифруется. В зашифрованном виде код постоянно хранится на внешнем носителе. В расшифрованном виде присутствует в оперативной памяти. При динамическом шифровании последовательно шифруются/дешифруются процедуры (или отдельные фрагменты) программы или критического участка программы;

- шифрование пароля. Этот метод упоминался выше;

- шифрование данных. Зашифрованные команды после дешифрации легко «узнать на вид», поэтому рекомендуется шифровать данные.

Сильной реализацией специалистами признается шифрование данных прямо в исходном тексте программы.

Методы для защиты условно-бесплатных программных продуктов. Среди таких методов выделим следующие:

- *защита с помощью серийного номера*. Предполагается наличие уникального номера в каждом экземпляре программы. При размножении программы в нее заносится её порядковый номер, который затем проставляется на регистрационной карточке продажи этой программы конкретному покупателю. При обнаружении копии программы у незарегистрированного пользователя можно найти источник похищения программы и даже проследить цепочку. По идеологии защита с использованием серийного номера близка к защите с помощью пароля;

- *регистрационные коды*. Разработчики предоставляют в распоряжение пользователя так называемую незарегистрированную версию – приложение, работающее либо в демонстрационном режиме, либо с ограниченными возможностями. После оплаты пользователь получает пароль и/или регистрационный номер, ввод которого обеспечивает работу приложения в полном объеме (версия приложения теперь называется зарегистрированной). При реализации такой защиты авторы идут в основном двумя путями. В первом случае введенный пароль или регистрационный номер просто сравниваются с эталоном. Во втором случае (более надежная защита) на основе пароля и/или реги-

страционного номера пользователя с помощью специальных механизмов (это чаще математические преобразования) генерируется регистрационный код. Приложение при этом дополняется модулем ввода пароля (регистрационного номера), механизмом генерации кода и сравнением полученного результата с оригинальным кодом;

- *ограничение по времени*. Ограничение по времени заключается в том, что пользователь имеет возможность бесплатно эксплуатировать ПО либо в течение определенного времени с момента первого запуска, либо просто ограничен датой (временем) последнего возможного запуска. В этом случае приложение дополняется функциями чтения текущей даты (времени) и сравнения с эталонными;

- *защита счетчиком установленных копий*. Некоторые фирмы продают диски с заранее обговоренным числом копий, которые можно получить с дистрибьюторского диска. Как правило, для такого продукта существует программа установки (инсталляции), которая при очередном копировании уменьшает счетчик числа копий. Если же основную программу скопировать без программы установки, то такая копия в лучшем случае не будет работать. Нельзя также скопировать и весь диск с установочной программой, так как программа установки проверяет оригинальность диска, на которой она записана. В основном такую защиту применяют на игровых программах. Этот вид защиты может сочетаться с защитой серийным номером;

- *раздражающие экраны (Nag Screen)*. Метод психологического воздействия на незарегистрированного пользователя с помощью вывода на экран сообщений, напоминающих пользователю о регистрации. Идея заключается в том, что такого рода сообщения выводятся в виде окон многократно на протяжении всего сеанса работы с приложением. Пользователю для продолжения работы приходится постоянно отключать эти окна, что отвлекает и раздражает его. Более интересной является реализация метода, когда для закрытия такого окна пользователю приходится нажимать каждый раз на разные клавиши или вводить длинные слова. Называют такую защиту Nag Screen - раздражающий экран (англ. nag - изводить, раздражать). Рассчитывают авторы на то, что постоянное раздражение пользователя либо заставит его отказаться от работы с приложением, либо заплатить за программный продукт и зарегистрироваться;

- *опрос пароля при загрузке программы*. Причем сам пароль не хранится в программе, а обрабатывается введенная строка и по полученному адресу вызывается следующая выполняемая подпрограмма. В случае ошибки вероятность верного входа ничтожно мала;

- *программная защита от дизассемблирования*. Практически любую защиту можно снять или обойти. Поэтому необходимо принять меры, чтобы для "взлома" программы требовались такие же затраты, как и на создание программы, подобной защищаемой, или же покупка программы была бы дешевле;

- *использование технических отличий в машине для программной защиты*. Как правило, каждая модель ПЭВМ имеет свои индивидуальные особенности. Это можно использовать для проверки уникальности компьютера, на котором установлена программа.

Наиболее распространенные **методы вскрытия**:

- *прямое построение по загрузочному модулю текста программы на ассемблере* или другом языке. После этого из текста удаляются подпрограммы проверки и строится заново загрузочный модуль. Недостаток - если исполняемые коды зашифрованы и расшифровываются лишь в момент исполнения, по загрузочному модулю практически невозможно восстановить его первоначальный вид на ассемблере;

- *в загрузочном модуле отладчиком прослеживается система защиты*, а затем в модуль вносятся такие изменения, чтобы соответствующая подпрограмма уже не смогла активизироваться. Недостаток - существуют приемы противодействия, прерывающие процесс дизассемблирования. На ПЭВМ большинство отладчиков используют для отладки стандартные прерывания. Если изменить векторы этих прерываний, исследование программы отладчиком становится затруднительным. Второй путь – передача управления в программе с помощью изменения указателя стека так, что отладчик не будет знать адрес следующей исполняемой программы;

- с помощью отладчика *программа загружается в ОЗУ, проходятся все ступени защиты и в момент завершения работы программы защиты на диск записывается копия ОЗУ*, чтобы в дальнейшем можно было загрузить с диска программу с пройденным этапом защиты. Недостаток - этот метод имеет смысл применять для программ

небольшого размера и только в том случае, если защита проверяется сразу, а не в середине работы и нет проверок в течение всего сеанса. Как правило, необходима полная информация о работе защиты (в частности долговременное наблюдение);

- *аппаратная трассировка с помощью внутрисхемных эмуляторов* или логических анализаторов с блоками для трассировки. Недостаток - нужна специальная дорогостоящая аппаратура и специалисты, умеющие с ней работать. Противодействие аналогично борьбе против отладчиков и дизассемблирования.

3.2. Программно-аппаратная защита

Программно-аппаратная защита используется для защиты программного обеспечения от несанкционированного (неавторизованного) доступа (НСД) и нелегального использования.

Защитный механизм программным образом опрашивает специальное устройство, используемое в качестве ключа, и работает только в его присутствии.

Ключ - это аппаратная часть системы защиты, представляющая собой плату с микросхемами памяти и в некоторых случаях микропроцессором, помещенную в корпус и предназначенную для установки в один из стандартных портов ПК (COMM, LPT, PCMCIA, USB) или слот расширения материнской платы. Также в качестве такого устройства могут использоваться смарт-карты.

Таким образом, механизм программно-аппаратной защиты содержит две составляющие:

- аппаратное устройство (аппаратная часть);
- программный модуль (программная часть).

Поэтому обычно говорят о системах программно-аппаратной защиты.

Очевидно, что стоимость такого механизма превышает стоимость программной защиты, причем стоимость аппаратной части, как правило, превышает стоимость программной части. По этой причине программно-аппаратная защита считается привилегией корпоративных заказчиков, так как для индивидуального пользователя часто неприемлема с экономической точки зрения.

Обратим внимание на то, что по существу программно-аппаратная защита не является защитой программ от нелегального распространения и использования. Не станет заказчик программы оплачивать дорогую аппаратуру только ради соблюдения авторских прав разработчика. Но если программный продукт снабжен модулем, предназначенным для защиты от НСД к данным и информации пользователя, то заказчик, как правило, готов платить за аппаратуру, повышающую надежность такой защиты.

Система защиты от НСД к данным реализована таким образом, что осуществляет проверку легальности пользователя при работе с программным обеспечением и тем самым косвенно препятствует и незаконному использованию программы.

Кроме того, современные аппаратные устройства (ключи) помимо информации о законном пользователе могут содержать также информацию о программном продукте. А системы программно-аппаратной защиты, кроме аутентификации пользователя, могут производить аутентификацию приложения.

Поэтому системы программно-аппаратной защиты от несанкционированного доступа могут служить в то же время и для защиты авторских прав разработчиков программ.

Системы программно-аппаратной защиты широко используются на практике и многими пользователями признаются надежным средством.

Рассмотрим основные моменты защиты информации от несанкционированного доступа. Речь идет о таком порядке работы, при котором:

- доступ к информации имеет только тот пользователь, который имеет разрешение, будем называть такого пользователя законным;

- каждый законный пользователь работает только со своей информацией и не имеет доступа к информации другого законного пользователя;

- каждый законный пользователь может выполнять только те операции, которые ему разрешено выполнять.

Для организации такого порядка работы прежде всего необходимо обеспечить распознавание законного пользователя. Этот процесс часто называют авторизацией пользователя.

Авторизация пользователя включает три этапа:

- идентификация пользователя;
- аутентификация пользователя;
- непосредственно авторизация пользователя.

Идентификация пользователя (identification) - это, с одной стороны, присвоение пользователю идентификатора - некоторого уникального признака (или нескольких); с другой – процесс, во время которого пользователь указывает присвоенный ему идентификатор. Другими словами, идентификация - это процесс, при котором пользователь называет себя.

Аутентификация пользователя (от англ. autentication - установление подлинности) - установление подлинности пользователя на основе сравнения с эталонным идентификатором.

Авторизация пользователя - установление прав пользователя. Авторизованный пользователь (авторизованное лицо) - пользователь (лицо), который получил определенные права на работу с информацией. В процессе авторизации для законного пользователя определяются права пользователя, то есть определяются данные, с которыми ему разрешено работать; операции, которые ему разрешено выполнять и т.п.

Идентификация пользователя может быть основана:

- на знании некоторой секретной информации (пароль, код);
- владении некоторым специальным предметом или устройством (магнитная карточка, электронный ключ);
- биометрических характеристиках (отпечатки пальцев, сетчатка глаза, спектральный состав голоса и т.п.).

Системы, основанные на знании некоторой секретной информации. К такого рода системам относятся прежде всего программные механизмы парольной защиты, которые были уже рассмотрены выше. Кроме того, заметим, что системы, основанные на владении некоторым специальным предметом или устройством (магнитная карточка, электронный ключ), как правило, предполагают также знание пользователем некоторой секретной информации.

Системы, основанные на владении некоторым специальным предметом или устройством. Традиционно в качестве таких устройств

применялись магнитные карточки. Система защиты снабжалась устройством чтения персональной информации (уникального кода пользователя), записанной на магнитной карточке. Заметим, что с точки зрения защиты от несанкционированного доступа такие системы обладают малой степенью надежности, так как магнитная карточка может быть легко подделана (например скопирована на специальном оборудовании).

Наибольшее распространение получили системы защиты, использующие смарт-карты (SmartCard - интеллектуальная карта). В памяти смарт-карты также хранится эталонная информация для аутентификации пользователя, но в отличие от традиционной магнитной карточки смарт-карта содержит микропроцессор, который позволяет производить некоторые преобразования уникального кода пользователя или некоторые другие действия.

Параллельно с развитием смарткарт-технологий усиленными темпами развиваются сегодня технологии, основанные на использовании электронных ключей. Такие технологии являются наиболее интересными с точки зрения защиты прав разработчиков программного обеспечения, поэтому ниже рассмотрим их подробнее.

Системы, основанные на биометрических характеристиках. Системы используют уникальные индивидуальные особенности строения человеческого тела для идентификации личности. В состав систем входят специальные считывающие устройства, генерирующие эталонные идентификаторы пользователей, а также устройства или программное обеспечение, анализирующее предъявленный образец и сравнивающее его с хранящимся эталоном.

В настоящее время разработаны разнообразные устройства, позволяющие идентифицировать личность на основе биометрических характеристик.

Устройства считывания отпечатков пальцев идентифицируют личность по форме и числу деталей - точек начала и конца линий на пальце.

Сканеры сетчатки глаза сканируют образцы сетчатки глаза пользователя, сосредоточиваясь на уникальных кровеносных сосудах. С помощью инфракрасного излучения берутся данные по 300 точкам в области сетчатки глаза, и собранная информация преобразуется в число.

Устройства верификации голоса строят математическую модель вокального диапазона говорящего и используют ее для сравнения с образцом голоса.

Устройства считывания геометрии руки используют свет для построения трехмерного изображения руки человека, проверяя такие характеристики, как длина и ширина пальцев и толщина руки.

Очевидно, что биометрические системы сложно реализуются, требуют хранения объемных баз данных, надежных технологий распознавания образов и дорогостоящей считывающей аппаратуры. Поэтому применяются такие системы защиты от несанкционированного доступа в основном в учреждениях, требующих особого контроля за доступом к секретной информации.

Аутентификация пользователя обычно реализуется по одной из двух схем:

- простая PIN-аутентификация;
- защищенная PIN-аутентификация.

Обе схемы основаны на установлении подлинности пользователя посредством сравнения PIN-кода пользователя (PIN - Personal identification number, персональный идентификационный номер) с эталоном.

При *простой PIN-аутентификации* PIN-код просто посылается в ключ (смарт-карту). Ключ (смарт-карта) сравнивает его с эталоном, который хранится в его (ее) памяти, и принимает решение о дальнейшей работе.

Процесс *защищенной PIN-аутентификации* реализуется по следующей схеме:

- защищенное приложение посылает запрос ключу (смарт-карте) на PIN-аутентификацию;
- ключ (смарт-карта) возвращает случайное 64-разрядное число;
- приложение складывает это число по модулю 2 с PIN-кодом, который ввел владелец ключа (смарт-карты), зашифровывает его DES-алгоритмом на специальном ключе аутентификации и посылает результат ключу (смарт-карте);
- ключ (смарт-карта) осуществляет обратные преобразования и сравнивает результат с тем, что хранится в его (ее) памяти.

В случае совпадения считается, что аутентификация прошла успешно и пользователь (приложение) может продолжать работу.

3.3. Идентификация программного обеспечения

В основе идентификации программного обеспечения лежит идея сопровождения каждого экземпляра (копии) программного продукта *скрытой информацией об управлении правами*. Впоследствии при наличии спора между потенциальными авторами (либо между автором и лицом, незаконно использующим программный продукт) подтвердить факт авторства можно, раскрыв информацию об управлении правами, внедренную в спорный экземпляр программного продукта.

Информация об авторском праве, внедренная в экземпляр (копию) программного продукта, должна быть скрыта, иначе нарушитель легко сможет устранить или изменить ее.

Таким образом, для предварительной защиты программного продукта автору необходимо решить три вопроса:

- о содержании информации об управлении правами;
- способе внедрения информации в каждый экземпляр продукта;
- методах сокрытия информации об управлении правами.

Содержанием информации об авторском праве может быть любая информация, идентифицирующая автора (разработчика), а также любая информация, идентифицирующая программный продукт (конкретную копию). В дальнейшем информацию об управлении правами будем называть коротко идентификатором программного продукта.

Коды, в которых представлена информация об управлении правами, будем называть идентификационными (авторскими) метками.

На практике разработчики в качестве идентификационной метки используют идентификатор автора. Это может быть текстовая информация с именем разработчика и/или авторский код, представляющий собой уникальное число. Кроме того, идентификатор может включать также адрес, e-mail, телефон и т.п. Программный продукт идентифицируется, как правило, названием, номером версии, датой выхода версии и другими характеристиками. Подчеркнем, что автор вправе использовать любую необходимую информацию.

Способ внедрения информации об управлении правами зависит, во-первых, от назначения, типа и формата программного продукта, во-вторых, от возможности скрыть информацию в программном продукте определенного формата.

Скрыть информацию об управлении правами, равно как и любую другую информацию, можно двумя путями. Первый путь - скрыть содержание информации. Отметим, что при этом факт наличия (передачи) информации остается известным. Второй путь - скрыть сам факт наличия (передачи) информации. Содержание при этом может быть открытым.

Сокрытие содержания информации (смысла) может быть произведено с помощью методов и алгоритмов криптографии. Другими словами, чтобы скрыть содержание информации, необходимо ее зашифровать.

Методы, с помощью которых можно скрыть факт наличия (передачи) информации, изучает *стеганография* (от греч. «тайнопись»). Методы и способы внедрения скрытой информации в файлы изучает компьютерная стеганография.

Необходимо обратить внимание, что в случае, когда для сокрытия информации об управлении правами применены только методы криптографии, злоумышленнику для устранения идентификатора достаточно просто обнулить байты, содержащие идентификатор, при этом нет необходимости вскрывать алгоритм или ключ шифрования. Следовательно, для надежного сокрытия информации об управлении правами необходимо скрыть сам факт использования защиты такого рода либо сделать неизвестным место, в котором записан идентификатор, то есть необходимо использовать прежде всего стенографические методы.

Применение компьютерной стеганографии для внедрения идентификационных меток в объектные коды обусловлено тем, что, во-первых, существует возможность видоизменить объектный код программы без потери ее функциональности, во-вторых, существует возможность внести определенное количество байтов, несущих информационную нагрузку.

Подчеркнем, что применение методов цифровой стеганографии для внедрения идентификационных меток весьма сомнительно: в отличие от данных, содержащих оцифрованное изображение или звук, которые могут быть до некоторой степени видоизменены без потери качества изображения или звука, коды и данные программы требуют абсолютной точности.

Методы компьютерной стеганографии:

- *внедрение в программы цифр и кодов, в которых представлена информация об управлении правами*. Механизмы основаны на наличии свободных участков в объектных кодах программ, хранящихся в исполнимых файлах (существуют свободные полностью или частично секторы файла; структуры заголовков файлов в формате EXE, Portable Executable, New Executable содержат зарезервированные поля; существуют пустоты между сегментами исполняемого кода и др.). Внедрение авторской информации в свободные участки, во-первых, гарантирует правильную работу изменяемого объектного кода программы, а во-вторых, не изменяет размер файла. При внедрении идентификационных меток в свободные участки в объектных кодах программ необходимо предотвращать возможность удаления идентификационных меток способом, при котором нарушитель без анализа конкретных мест внесения метки может просто «обнулить» все имеющиеся свободные участки;

- *способы изменения объектных кодов*, базирующиеся на положении о том, что объектный код содержит информацию (описательного характера), модификация которой также не приведет к потере правильного функционирования программы. Так, например, форматы выполнимых файлов (EXE, Portable Executable, New Executable) таковы, что изменение значений некоторых полей не скажется на выполнении программы. Кроме того, объектные коды содержат текстовую информацию, изменение которой никак не повлияет на работу программы;

- *методы, которые базируются на вирусной технологии внедрения в выполнимые файлы*. В частности, можно дополнить объектный код программы некоторым модулем (набором команд, фрагментом кода), изменив при этом соответствующие характеристики (параметры) файла. Например, приписав информацию об управлении правами в конец файла в формате типа EXE, необходимо изменить значение поля длины файла в его заголовке. Можно внедрить в объектный код модуль, осуществляющий проверку наличия информации об управлении правами перед загрузкой программы, и не выполнять программу в случае модификации и/или удаления идентификацион-

ной метки. При этом необходимо изменить значение поля длины файла, а также точку входа в таблице настройки адресов и т.п.

Итак, существует достаточно способов для внедрения в программу скрытой информации об управлении правами. Заметим, что использование оригинальных алгоритмов и приемов, а также недокументированных возможностей операционной системы повысит надежность защиты.

Механизм защиты, основанный на использовании методов двух защитных дисциплин - криптографии и компьютерной стеганографии, - является более эффективным по сравнению с механизмом, использующим методы только одной защитной дисциплины.

Информация об управлении правами легко может быть закодирована в текстовых и HTML-файлах. Например, для текстовых файлов можно использовать метод скрытых гарнитур шрифтов: необходимо в очертаниях символов текста сделать малозаметные искажения, которые будут нести смысловую нагрузку. В HTML-файлы в конец каждой строки можно добавить определенное число пробелов, кодирующих идентификатор или сообщение, которое необходимо скрыть.

Электронно-цифровая подпись. Многие специалисты в качестве средства защиты прав автора на компьютерные программы называют электронную цифровую подпись.

Электронная цифровая подпись используется при передаче информации в компьютерных сетях для аутентификации автора (создателя) передаваемой информации и, кроме того, служит для доказательства (проверки) того факта, что подписанное сообщение или данные не были модифицированы.

Электронная цифровая подпись строится на основе двух компонент: во-первых, содержания информации, которая подписывается, во-вторых, личной информации (код, пароль, ключ) того, кто подписывает. Очевидно, что изменение каждой компоненты приводит к изменению электронной цифровой подписи. Большинство алгоритмов создания электронной цифровой подписи основаны на шифровании с открытым ключом.

При использовании электронной цифровой подписи для защиты авторских прав на компьютерные программы необходимо учитывать,

что электронная цифровая подпись только тогда может выступать в качестве информации об авторском праве на компьютерную программу, если она приложена к каждому экземпляру (копии) программы.

3.4. Контрольные вопросы, задания, темы рефератов

А. Контрольные вопросы

1. Что представляют собой системы, основанные на знании некоторой секретной информации?
2. Что представляют собой системы, основанные на владении некоторым специальным предметом или устройством?
3. Какую программную защиту можно считать надежной?
4. Как строится «парольная защита» ПО?
5. Дайте определение терминам: шифрование, дешифрование.
6. Какие виды криптосистем вам известны?
7. Каковы механизмы защиты программ на основе шифрования?
8. Каков механизм защиты с помощью серийного номера?
9. Как работает программно-аппаратная защита?
10. Каковы способы внедрения информации об управлении правами?

Б. Задания

1. Перечислите наиболее известные криптографические методы.
2. Приведите и подробно рассмотрите методы для защиты условно-бесплатных программных продуктов.
3. Приведите примеры наиболее распространенных программных продуктов по защите программного обеспечения.
4. Сформулируйте основные требования к программно-аппаратным продуктам, предназначенным для защиты ПО.
5. Проанализируйте современный рынок программно-аппаратных средств по защите авторских прав на ПО.

В. Темы рефератов

1. Парольная защита как один из базовых методов защиты от незаконного использования программ.
2. Шифрование как один из базовых методов защиты от незаконного использования программ.

3. Идентификация и аутентификация пользователя.
4. Методы компьютерной стеганографии.
5. Методы вскрытия программных средств защиты.
6. Рассмотрите и опишите системы, основанные на биометрических характеристиках.
7. Скрытая информация об авторском праве. Методы внедрения.
8. Электронно-цифровая подпись.

ЗАКЛЮЧЕНИЕ

Необходимость правовой охраны программного обеспечения вытекает из все большего проникновения информационных технологий в жизнь общества. Право должно соответствовать сложившимся общественным отношениям – в соответствии с данной аксиомой программы для ЭВМ в 70-х годах двадцатого века, когда началось их сравнительно массовое применение, были включены в перечень объектов интеллектуальной собственности, подлежащих правовой охране. Программы для ЭВМ и базы данных изначально были отнесены к объектам авторско-правовой охраны. Данное положение обусловлено рядом причин, среди которых прежде всего выделяются экономические. Авторско-правовая охрана программ для ЭВМ оперативнее, дешевле и демократичнее по сравнению с их охраной нормами патентного законодательства, для которой характерна сложность экспертизы на мировую новизну, длительность процедуры патентования, нецелесообразность в ряде случаев публикации описания программ. Кроме того, сказались последствия формирования единого мирового рынка и взаимозависимость национальных экономических систем, императивы международного сотрудничества и международной конкуренции. Тенденция к формированию действенного режима правовой охраны программ для ЭВМ на основе авторского права в рамках мировой экономической системы приобрела доминирующий характер. Ни изменить ее, ни отказаться от следования в фарватере соответствующего политического курса отдельные страны уже не в состоянии. Это в полной мере относится и к Российской Федерации.

В России существует один из самых высоких в мире уровней пиратства – 88 %. Причин здесь несколько. Отчасти это происходит потому, что еще в СССР ПО в принципе не воспринималось как товар и даже не рассматривалось в качестве объекта авторского права. Только в 1996 г. появился первый юридический прецедент: фирма «1С» выиграла у одного из пиратов судебный процесс, который тянулся почти год, и в результате которого фирма-нарушитель прекратила незаконную торговлю и по требованию конкретных покупателей вернула деньги тем, кто купил поддельные программы.

Следующая причина - экономическая. Общеизвестно, что уровень компьютерного пиратства напрямую связан с уровнем доходов на душу населения. В США и Западной Европе, где уровень доходов на душу населения максимальный, - уровень пиратства минимальный.

Следует подчеркнуть, что под термином «компьютерные пираты» понимаются все звенья цепочки: производители пиратских дисков - продавцы - пользователи. К тому же те, кто производит и продает пиратскую продукцию, обычно лучше осведомлены о том, что они нарушают закон, и в социологических опросах на подобные темы обычно не участвуют. А вот пользователи пиратского софта подчас считают, что они никакого криминала не совершают. Таким пользователям еще раз следует напомнить, что сам факт использования пиратского ПО является пиратством, что использовать ПО можно только с разрешения автора и что нарушение данного правила влечет за собой наказание.

Особо следует остановиться на производстве программ нашими отечественными разработчиками. Далеко не все отдают себе отчет в том, что ПО, созданное на базе нелегально приобретенного средства разработки, тоже, в свою очередь, становится нелегальным товаром. Даже если вы от начала до конца написали код некоторой программы, но использовали ворованный компилятор, вы произвели нелицензионный товар. А если вы продаете данный товар покупателю, то и он становится обладателем ворованного продукта. О предусмотренных законом наказаниях наши граждане имеют самое приблизительное представление.

Следует напомнить, что согласно ст. 146 части второй УК РФ за использование пиратской продукции в качестве наказания может фигурировать штраф до 400 МРОТ или лишение свободы на срок до пяти лет. Руководителя предприятия, которое ведет бизнес с использованием нелицензионного софта, можно также привлечь за неуплату налога. Естественно, если ПО приобретено нелегально, то обычно налог не уплачен, а это подпадает под ст. 199 УК РФ, которая предусматривает для руководителей организаций, уклоняющихся от уплаты налогов путем включения в бухгалтерские документы заведомо искаженных данных о доходах или расходах, либо иным способом, нака-

зание в виде лишения права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет либо лишение свободы на срок до четырех лет.

Конечно, сам факт принятия закона не решает проблемы. У государства либо нет сил и средств на борьбу с пиратством, либо эта проблема не признается им как первоочередная.

Что разработчики могут противопоставить массовым нарушениям? Исходя из зарубежного и отечественного опыта, наряду с применением технических средств защиты авторского права могут быть использованы иные подходы, позволяющие уменьшить отрицательное влияние пиратства на бизнес, в частности:

- *пропаганда*, которая заключается в демонстрации достоинств лицензионной продукции и разъяснении недостатков пиратских копий, организации PR-кампаний в СМИ по проблемам компьютерного пиратства и т.д.;

- *обучение*, проведение тематических семинаров, конференций, публикация методической и справочной литературы, позволяющей пользователю избрать менее затратные, но вместе с тем законные способы приобретения ПО;

- *силовые методы*, или юридический путь, который основывается на выявлении производителей и распространителей нелегальной продукции и привлечении их к уголовной или административной ответственности. Такие процедуры невозможны без активного участия правоохранительных органов государства: подразделений МВД, прокуратуры, антимонопольной и таможенной служб, судебной системы.

Не всегда приемлемыми оказываются для производителей методы ценовой борьбы с "пиратами". В условиях, когда распространители пиратских копий избавлены от несения расходов, связанных с начальным этапом жизненного цикла программ (проектирование, кодирование, тестирование, маркетинговые мероприятия, связанные с выводом продукта на рынок), ценовая конкуренция с ними практически невозможна. Абсолютно неприменима она к программным продуктам делового назначения ввиду того, что при достаточно большой себестоимости разработки и поддержки таких продуктов их тиражи относительно невелики (по сравнению с программами домашнего назначения). Впрочем, добросовестная конкуренция невозможна с любыми

субъектами, изначально строящими свою коммерческую деятельность на противоправной основе.

С ростом темпов информатизации современного общества растет роль программ для ЭВМ и баз данных как основных составляющих данного процесса и их эффективная правовая охрана будет способствовать ускорению общего научно-технического прогресса в мире.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК*

1. Бернская конвенция по охране литературных и художественных произведений» от 09.09.1886 (ред. от 28.09.1979) // Бюллетень международных договоров. – 2003. – № 9.
2. Гаврилов, Э. П. Вступительная статья / Э. П. Гаврилов // Закон РФ "Об авторском праве и смежных правах". – М. : БЕК, 1995. – С. I - XXV.
3. Гаврилов, Э. П. Общие положения права интеллектуальной собственности: краткий комментарий к гл. 69 ГК РФ / Э. П. Гаврилов // Хозяйство и право. – 2007. – № 9. – С. 51.
4. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.06 № 230-ФЗ (принят Гос. думой РФ 24.11.06) (ред. от 30.06.08) // Собрание законодательства РФ. – 2006. – № 52.
5. Директива Совета Европейского Сообщества от 14 мая 1991 г. № 91/250/ЕЕС «О правовой охране программ для ЭВМ» // Международное частное право: сб. докл. / сост. : К.А. Бекяшев, А.Г. Ходаков. – М. : БЕК, 1997. – С. 342 – 357.
6. Закон Российской Федерации "Об авторском праве и смежных правах" от 09.07.93 № 5351-1 (ред. от 20.07.04) (утратил силу с 1.01.08) // Российская газета. – 1993. – № 147.
7. Закон Российской Федерации "О правовой охране программ для электронных вычислительных машин и баз данных" от 23.09.92 № 3523-1 (ред. от 02.02.06) (утратил силу с 1.01.08) // Российская газета. – 1992. – № 229.
8. Как защитить интеллектуальную собственность в России: Правовое и экономическое регулирование: справ. пособие / под ред. А. Д. Корчагина. – М. : ИНФРА–М, 1995. – 335 с.

* Печатается в авторской редакции.

9. Комментарий к законодательству об охране интеллектуальной собственности: сб. / под общ. ред. В. И. Еременко. – М. : Фонд «Правовая культура», 1997. – 235 с.
10. Закон Российской Федерации "О правовой охране программ для электронных вычислительных машин и баз данных" № 3523-1 (принят Верховным Советом Российской Федерации 23.09.92 г.) // Ведомости съезда народных депутатов РФ и Верховного Совета РФ. – 1992. – № 42. – Ст. 2325.
11. Закон Российской Федерации "Об авторском праве и смежных правах" № 5351-1 (принят Верховным Советом Российской Федерации 09.07.93) // Ведомости съезда народных депутатов РФ и Верховного Совета РФ. – 1993. – № 32. – Ст. 1242; Собрание законодательства РФ. – 1995. – № 30. – Ст. 2866.
12. Постановление Верховного Совета Российской Федерации от 09.07.93. № 5352 – 1 «О порядке введения в действие Закона Российской Федерации "Об авторском праве и смежных правах" // Ведомости съезда народных депутатов и Верховного Совета РФ. – 1993. – № 32.
13. Правила составления, подачи и рассмотрения заявок на официальную регистрацию программ для ЭВМ и баз данных. Приказ Российского агентства по правовой охране программ для ЭВМ, баз данных и топологий интегральных микросхем от 05.03.93 // Сборник нормативных документов по авторскому праву. – М. : Статут, 1995. – С. 234 – 245.
14. Хаметов, Р. Каким быть авторскому договору? / Р. Хаметов // Интеллектуальная собственность. – 1997. – № 3 / 4. – С. 53 – 60.
15. Шамхолова, Н. А. Программы для ЭВМ как служебные произведения / Н.А. Шамхолова // Патенты и лицензии. – 1999. – № 6. – С. 36 – 41.
16. Интернет http://dostup1.ru/society/society_495.html
17. Интернет http://infolex.narod.ru/gpl_gnu/gplrus.html
18. Интернет http://linux.mykostroma.ru/index.php?topic=113.0
19. Интернет http://ns.edison.ru/magazins/www.pcweek.ru/97_12/win
20. Интернет http://ru.wikipedia.org/wiki/Открытое аппаратное обесп.
21. Интернет http://sud.fstore.ru/

22. Интернет http://www.appp.ru/
23. Интернет http://www.appp.ru/obmen/materiali/2007/22-6.htm
24. Интернет Интернет http://www.gnu.org/copyleft/copyleft.ru.html
25. Интернет http://www.gnu.org/philosophy/free-sw.ru.html
26. Интернет http://www.intuit.ru/department/history/law
27. Интернет http://www.libertarium.ru/libertarium/minimal-theses
28. Интернет http://www.mosreg.ru/news/31000.html
29. Интернет http://www.mvd.ru/press/release/5405/
30. Интернет http://www.optim.ru/sergo1.asp.htm
31. Интернет http://www.relcom.ru/win/Internet/ComputerLaw/comm.htm
32. Интернет http://www.relcom.ru/win/Internet/ComputerLaw/Judge.htm
33. Интернет http://fravia.anticrack.de
34. Интернет www.ifap.ru
35. Интернет http://infonet.cherepovets.ru/citforum/security/articles/plan/

ОГЛАВЛЕНИЕ

Учебное издание

Комплексная защита объектов информатизации. Книга 17

МОНАХОВ Михаил Юрьевич
ТАШМУХАМЕДОВА Валерия Фароговна

ЗАЩИТА АВТОРСКИХ ПРАВ НА ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Актуальные вопросы информационного права

Учебное пособие

Подписано в печать 00.05.09.
Формат 60x84/16. Усл. печ. л. 3,49. Тираж 100 экз.
Заказ
Издательство
Владимирского государственного университета
600000, Владимир, ул. Горького, 87.