ванных методов совпадает, поэтому для иллюстрации эффективности оптимизации приведем только график отношения величины приращения к величине суммарной длины связей.

Рис.4. Результаты исследования алгоритмов размещения

Заключение. Проведенные исследования позволили модифицировать алгоритм размещения и уменьшить его вычислительную сложность до величины $O(n^2)$. Предложенный подход к вычислению приращения суммарной длины связей как суммы частичных приращений, вносимых различными подобластями области размещения, также может быть применен для алгоритмов групповой перестановки, а также для оптимизации размещения в 3D-области.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Курейчик В.М.* Математическое обеспечение конструкторского и технологического проектирования с применением САПР. – М.: Радио и связь, 1990.
2. *Кормен Т., Лейзерсон И., Ривест Р.* Алгоритмы: построения и анализ. – М.: МЦМО, 2000.
3. Sherwani Naveed. Algorithms for VLSI Physical Design Automation, Kluwer Academic Publishers, Boston/Dordrecht/London, 1995.
4. *Г Гэри М., Джонсон Д.* Вычислительные машины и труднорешаемые задачи. – М.: Мир, 1982.

В.М. Глушань, Р.В. Иванько, Р.М. Романов, М.Д. Сеченов

ПРАВОВЫЕ АСПЕКТЫ ПОСТРОЕНИЯ И ИСПОЛЬЗОВАНИЯ РАСПРЕДЕЛЕННЫХ САПР

Введение. Концепция распределенных вычислительных систем (РВС) появилась около четверти века назад и базируется она на понятии процессорной группы, впервые введенного разработчиками экспериментальной распределенной операционной системы MEDUSA в 1980 году [1]. Под этим термином понимается множество процессов, взаимодействующих для согласованного решения общей задачи. Справедливости ради следует заметить, что концепция параллельных вычислений на многопроцессорных вычислительных структурах (МВС) появилась гораздо раньше, а для САПР она воплотилась в специализированные моделирующие

структуры. Некоторые подходы к реализации этих структур изложены в монографии [2].

Однако следует отметить, что если цели у РВС и МВС одни и те же – повышение производительности, то сущность их различна. РВС по определению являются распределенными, а МВС сосредоточенными, т.е. всегда локальны – иначе говоря, все структурные составляющие МВС сосредоточены в одном локальном месте (помещении). Из этих различий вытекают и проблемы РВС, отсутствующие у МВС. Одной из таких достаточно острых проблем является правовая проблема. Существующим путям решения этой проблемы в настоящее время, правовым тонкостям в их преодолении посвящена эта статья.

1. Сущность правовой проблемы распределенных САПР. Для того, чтобы уяснить сущность проблемы, необходимо рассмотреть вопрос об организационных особенностях структуры различных видов САПР нашли широкое распространение в самых различных областях деятельности (проектировать можно что угодно) и, как следствие, классифицируются по многим признакам. Но нас будет интересовать разновидности САПР, различающиеся по *территориальному признаку*. По этому признаку САПР можно разделить на *нераспределенные и распределенные*. К нераспределенным будем относить традиционные одно-компьютерные САПР. К распределенным САПР отнесем такие, в решении задач проектирования которых используется не отдельный компьютер или рабочая станция, а некоторое их количество, объединенных сетью – локальной, корпоративной, региональной и, возможно, глобальной – Интернет [3].

В нераспределенной САПР средство проектирования (компьютер и периферийное оборудование) полностью находятся в распоряжении проектировщика. В распределенных же САПР средством проектирования является множество рассредоточенных по сетям компьютеров, некоторые из которых принадлежат локальной сети разработчика, а некоторые – другим сетям, которые для проектировщика являются «чужими». А как можно использовать «чужие» компьютеры? Для этого существует две возможности: легальная и нелегальная.

Легальная возможность возникает в том случае, когда распределенная САПР строится на основе только локальной сети проектировщика без использования «чужих» компьютеров или с выходом в другие сети, но с заключением предварительных договоров на использование их компьютеров. Легальная возможность надежна, но имеет существенные практические ограничения в повышении производительности САПР. Это вызвано тем, что заключить предварительные договора на использование большого количества компьютеров (фактически взять в аренду) других сетей достаточно сложно. Если иметь в виду региональные сети, а тем более глобальную, то это мероприятие является практически невозможным.

В то же время, как показано в [3], распределенная САПР будет эффективной, если она может использовать десятки, сотни, а то и тысячи компьютеров. А это возможно лишь в том случае, если проектировщик может подключиться к региональной сети или даже сети Интернет. Но, если сделать это легально практически невозможно, то возникает идея нелегального использования компьютеров региональных и глобальной сети Интернет. Тогда, по существу, мы будем иметь виртуальную САПР. При этом на первый план выдвинутся вопросы использования «чужих» компьютеров и вопросы надежности функционирования виртуальной САПР. Вопросы надежности имеют самостоятельную сущность. Здесь же мы рассмотрим правовые вопросы построения и использования виртуальных САПР.

2. Законодательные акты в области информатизации общества. Итак, из сказанного выше следует, что под распределенной САПР авторы понимают такую,

в которой «чужие» компьютеры используются легально, т.е. вполне законно на основании заключенных договоров. В виртуальных же САПР число используемых «чужих» компьютеров будет существенно больше, чем в распределенных, причем некоторые из них будут нелегальными. В них проектирующее программное обеспечение будет внедряться нелегально, без согласования с владельцем. Поэтому возникает вопрос о правовой законности такого внедрения. Рассмотрим статьи законов Российского законодательства, под которые может подпадать данное действие.

Компьютерным преступлениям в Уголовном кодексе РФ посвящен раздел «О правовой охране программ для ЭВМ и баз данных» главы 28 [4]. В этом разделе представлены три статьи: статья 272 – неправомерный доступ к компьютерной информации; статья 273 – создание, использование и распространение вредоносных программ для ЭВМ; статья 274 – нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети.

Статья 272 рассматривает возможные случаи неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, систем ЭВМ или их сети.

По делам, квалифицируемым данной статьей как преступление, должно быть установлено, что компьютерная информация, к которой осуществлен доступ, охраняется законодательством о государственной тайне, о собственности, об авторском праве или др., что самим фактом несанкционированного к ней доступа нарушены прерогативы государства, права собственника, владельца, автора или другого юридического или физического лица.

Неправомерными действиями в статье признается доступ в закрытую информационную систему лица, не являющегося законным пользователем, либо не имеющего разрешения для работы с данной информацией.

Несанкционированное проникновение к органам управления ЭВМ или в сеть ЭВМ следует рассматривать как приготовление к доступу к компьютерной информации.

Данная статья уголовного кодекса предусматривает ответственность за неправомерный доступ к информации, только, если она запечатлена на машинном носителе, в ЭВМ, системе ЭВМ или их сети. Таким образом, данная норма уголовного законодательства оберегает компьютерную информацию, где бы она ни содержалась и ни циркулировала: в памяти ЭВМ, в каналах связи, на магнитных носителях.

Статья 273 предполагает уголовную ответственность за создание, использование и распространение вредоносных программ для ЭВМ, получивших в среде специалистов по информатике более распространенный термин компьютерный вирус. Данная статья квалифицирует соответствующее деяние как преступление в случаях:

- создание программы для ЭВМ, заведомо приводящей к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы аппаратной части;
- внесение в существующие программы изменений, обладающих аналогичными свойствами;
- использование двух названных видов программ;
- распространение программ, использование и распространение машинных носителей с программами, перечисленными выше.

Мера ответственности за каждое из описанных деяний зависит от тяжести последствий, повлекших данным преступлением, и карается лишением свободы от 3 до 7 лет.

Целью действия статьи 274 является предупреждение применения пользователями своих профессиональных обязанностей, влияющих на сохранность хранимой и перерабатываемой информации. Непосредственным объектом преступления, предусмотренным этой статьей, являются отношения по соблюдению правил эксплуатации ЭВМ, систем ЭВМ или их сетей, т.е. аппаратно-технического комплекса.

Применительно к данной статье под сетью понимается только внутренняя сеть ведомства или организации (локальная), на которую может распространяться ее юрисдикция. В глобальных сетях типа Интернет отсутствуют общие правила эксплуатации, их заменяют этические «Кодексы поведения», нарушения которых не могут являться основанием для привлечения к уголовной ответственности.

Поскольку в данной статье затрагиваются вопросы о нарушении правил эксплуатации аппаратно-технического комплекса ЭВМ, их систем и сетей на их основе, то данная статья преследует лишь те правонарушения, которые связаны с угрозой безопасности хранимой в ЭВМ и охраняемой законом информации.

Мы привели и обобщенно рассмотрели три основные статьи Российского законодательства в области правовой охраны программ для ЭВМ и баз данных. Более тщательный анализ этих статей позволяет заключить, что в них нет ни одного непосредственного ограничения по использованию «чужих» компьютеров в распределенных и виртуальных САПР. Есть лишь предпосылка к тому, что такое использование «чужих» компьютеров может быть инкриминировано по своему действию аналогично компьютерным вирусам. Но это возможно будет лишь в том случае, если внедряемые в «чужие» компьютеры проектирующие программы будут приводить к последствиям, аналогичным компьютерным вирусам.

Заключение. Российское законодательство по современным вопросам информатизации общества еще очень молодо. Ему еще не исполнилось и 15 лет. Поэтому оно еще не накопило достаточно прецедентов, которые необходимо ввести в правовое русло. Существующие же статьи законов предоставляют широкое поле законной деятельности для построения и использования распределенных САПР. Необходимо лишь следить за тем, чтобы внедряемое в «чужие» компьютеры программное обеспечение не наносило им материального ущерба. В связи с этим на передний план построения и использования распределенных САПР выдвигаются вопросы их надежного функционирования и связанные с ним смежные вопросы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *J. Ousterhout* et.al MEDUSA: an experiment in distributed operating structure//Comm. ACM. – 1980. – Vol.23., No.2. pp. 92–105.
2. *Курейчик В. М., Глушань В. М., Щербаков Л. И.* Комбинаторные аппаратные модели и алгоритмы в САПР. – М.: «Радио и связь», 1990. – 216 с.
3. *Глушань В. М., Иванько Р. В.* Анализ эффективности распределенных САПР//Известия ТРТУ. Тематический выпуск «Интеллектуальные САПР». – Таганрог: Изд-во ТРТУ, 2006, №8. – С. 115-120.
4. Уголовный кодекс РФ. 23 сентября 1992. (в ред. Федеральных законов от 02.11.2004 №127-ФЗ).