ким образом, требуется точная идентификация спектра $D_f(d_M^{эф})$ для каждого полимера.

4) Имеющиеся в литературе величины (ε/k) и d_M могут иметь достаточно широкий разброс (для одного и того же газа они могут различаться в 1,5-2,0 раза). Поэтому важно иметь более точные методы оценки эффективных величин этих параметров.

5) Указанная точность необходима, поскольку характерной особенностью всех скейлинговых и фрактальных соотношений является степенная зависимость, существенно повышающая погрешность расчета.

6) Степень связности структуры полимера, характеризуемая величиной d_s, существенно влияет на величину α_{ik}. Так, увеличение d_s от 1,0 для линейных полимеров до 1,33 для сшитых при прочих равных условиях увеличивает α_{ik} в среднем в 1,5 раза. Поэтому следует использовать точную величину этой размерности.

Проблемы передачи и обработки информациии

ПОДХОД К СИСТЕМНОМУ АНАЛИЗУ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Бочкарева Ю.Г., Смогунов В.В.,
Фунтиков В.А., Чижухин Г.Н.

Рассмотрим общую постановку вопроса системного анализа информационной безопасности АСОИ (автоматизированной системы обработки информации). Для такого анализа необходимо представить некоторую *систему* [1] *информационной безопасности* (СИБ), состоящую из *компонентов*, каждый из которых есть множество относительно однородных *элементов*, объединенных функциями для обеспечения выполнения общих целей функционирования СИБ. При этом понятие системы здесь не сводится к сумме компонентов, которые при объединении в систему выступают и, соответственно, воспринимаются как единое целое. Для СИБ имеют место следующие компоненты:

– стратегии (способы) *защиты* информации,

– стратегии (методы) прогнозирования *нападения* на рассматриваемый объект,

– механизмы принятия решения, использующие результаты обоих стратегий и представляющие собой *политику безопасности* (набор норм, правил и практических приемов, регулирующих управление и распределение ценной информации [2]).

Элементы СИБ – условно неделимая, самостоятельно функционирующая часть системы и, например, для первой компоненты это будут (как показано ниже) четыре стратегии защиты. Все компоненты объединяются общей функциональной средой.

Функциональная среда СИБ есть характерная для нее совокупность законов, алгоритмов и параметров, по которым осуществляется взаимодействие (обмен, взаимоотношение) между компонентами системы, а также функционирование (стабильность или деградация) системы в целом.

И, наконец, *структура* СИБ подразумевает совокупность связей, по которым обеспечивается информационный обмен между компонентами системы, определяющий функционирование ее в целом и способы взаимодействия ее с внешней средой.

Рассмотрим, для примера, подробней компоненты и элементы СИБ, из которых они состоят. Например, организация защиты информации [3] в самом общем виде может быть сформулирована как задача поиска оптимального компромисса между *потребностями в защите* и *необходимыми ресурсами* для этих целей. Потребности обусловлены важностью и объемами защищаемой информации, условиями ее хранения, обработки и использования. Ресурсы могут быть ограничены заданным пределом либо определяются условием обязательного достижения требуемого уровня защиты. В первом случае защита организуется так, чтобы при выделенных ресурсах обеспечивался максимальный уровень защиты, а во втором - уровень защиты обеспечивает минимальное расходование ресурсов.

Нетрудно видеть, что сформулированные случаи есть не что иное, как прямая и обратная постановки оптимизационных задач. Они достаточно детально изучены с помощью методов современной теории систем, информатики и прикладной математики. Однако имеющиеся неопределенные ситуации, а также, прежде всего, в данном случае невозможность получения функциональных зависимостей между объемом затрачиваемых ресурсов и достигаемым уровнем защиты не позволяют строго решить эти задачи подобными известными методами. Поэтому в целях создания условий для ориентации в этих неопределенных ситуациях и вводится понятие *стратегии защиты*. Под ней понимается системный взгляд на сложившуюся ситуацию, который распространяется и на системный подход к принятию наиболее рационального решения в этой ситуации. Количество таких стратегий должно быть небольшим (чтобы просто было бы ориентироваться в самих стратегиях), но в то же время должно полно и достаточно адекватно отображать всю гамму потенциально возможных ситуаций.

В этом смысле хороший урок преподает природа, которая имеет всего четыре стратегии защиты: 1) *оборонительная* или пассивная защита (надевание «брони»), например, черепаха - на себя или охранная территория – на окружающую среду; 2) *наступательная* или активная защита, выражающаяся в нападении и уничтожении нападающего (в том числе и с помощью вирусов); 3) *пространственно-временная* или защита с помощью изменения месторасположения в пространстве (например, бегство в пространстве от нападающего или перемещение в другую область адресного пространства ЗУ) или во времени (размножение – создание собственных копий); 4) *содержательная* или защита с помощью внесения изменений

в содержание объекта защиты или окружающей его среды (хамелеон меняет свой цвет, а дымовая завеса на флоте изменяет окружающую среду).

Все подобные стратегии защиты необходимо применять и в АСОИ. Однако защищающемуся объекту недостаточно владеть даже всеми четырьмя стратегиями защиты. Он должен уметь прогнозировать развитие событий. Поэтому вводится понятие *абсолютной системы защиты* [4], в которой работает и стратегия прогнозирования, способная в любой момент спрогнозировать наступление угрожающего события за время, достаточное для приведения в действие любой из адекватных стратегий защиты. Любая защищающаяся СИБ (отдельно взятый человек, государство, банк и т.п.) должна на основе анализа информации о текущих событиях внутри и вне системы определить (идентифицировать) прогнозируемое событие и принять решение какую стратегию защиты реализовать.

СПИСОК ЛИТЕРАТУРЫ

1. Д.М. Хомяков, П.М. Хомяков. Основы системного анализа. – М.: Изд-во механико-математического факультета МГУ им. М.В.Ломоносова, 1996 – 108 с.

2. А.А. Грушо, Е.Е. Тимонина. Теоретические основы защиты информации. – М.: Изд-во Агентства «Яхтсмен», 1996 – 192 с.

3. Г.Н. Чижухин. Основы защиты информации в вычислительных системах и сетях ЭВМ: Учеб. пособие.–.Пенза: Изд-во Пенз. гос. ун-та , 2001.–164 с.

4. С.П. Расторгуев. Абсолютная система защиты.// Системы безопасности связи и телекоммуникаций–№3, 1996,–с.86-88.

СТОХАСТИЧЕСКАЯ МОДЕЛЬ ОПТИМИЗАЦИИ МОНИТОРИНГА ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Кравец О.Я., Севрюков Н.Н.

В качестве модели телекоммуникационной сети удобно использовать сеть систем массового обслуживания (СМО), в которой каждый канал представляется двумя обслуживающими устройствами СМО, а узлы сети задают коммутационные матрицы для связи параметров потоков.

Входящими параметрами для узла являются интенсивности потоков $\lambda_{i,j}$, где i – индекс узла, откуда поступил поток, а j – индекс принимающего узла. Разные узлы имеют не одинаковое количество входов/выходов, обозначим их число через m_i, где i – индекс узла. Также характеристикой узла являются плотности потоков после коммутации – $\rho_{i,kl}$, где i – индекс узла, а k, l – вход/выход через которые проходит поток(см. рис.1). Тогда интенсивность потока с i-го узла на j-ный можно представить в виде:

$$l_{ij} = \sum_{k=1}^{m_i} r_{i,f(k,i)j}\, l_{f(k,i),i}\,, \qquad (1)$$

где $f(i_1,i_2)$ функция, которая задает распределение индексов входов/выходов, по сути, введена, чтобы не заострять внимание на выборе порядка их нумерации. Таким образом, было проведено суммирование по всем входам/выходам.

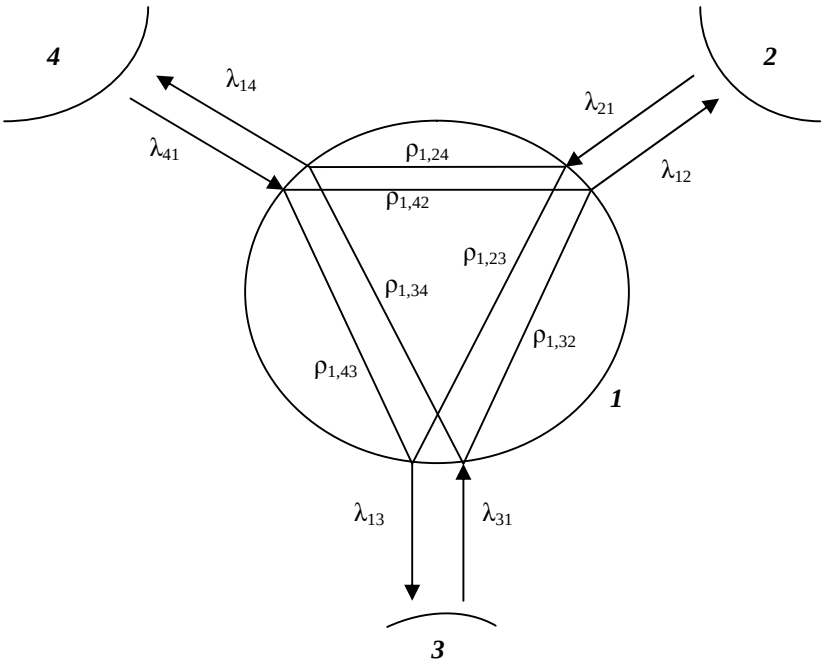

Рисунок 1. Характеристикой узла