УДК 681.324

СРАВНИТЕЛЬНЫЙ АНАЛИЗ РЕЗУЛЬТАТОВ РАЗЛИЧНЫХ ПОДХОДОВ К МОДЕЛИРОВАНИЮ СИСТЕМЫ ЗАЩИТЫ И НФОРМАЦИИ В РАСПРЕДЕЛЕННЫХ СЕТЯХ ОБСЛУЖИВАНИЯ

Б.Г. Исмайлов

Аннотация: Проведены сравнительный анализ результатов математических и имитационных методов решения задачи определения оптимальной программно-технической структуры систем защиты информации. Анализ результатов показывает, что они отличаются в пределах (2-10)%, а степень адекватности аналитической модели к исследуемому объекту увеличивается с уменьшением нагрузки сети.

Abstract: Comparison of mathematical and simulation methods to finding the optimal structure of systems of information protecting are carried out. Analysis of the results of the both methods shows that they differ in the interval of 2-10% and adequacy of analytical model increase with decreasing network’s load.

Актуальность проблемы

В данной работе проводится сравнительный анализ результатов различных подходов к решению проблемы определения оптимальной программно-технической структуры систем защиты информации (СЗИ) [1]. Такие системы создаются между различного рода распределенными сетями - с одной стороны и глобальной сетью с другой. Они инспектируют и фильтруют проходящие через них информацию. Это своего рода межсетевой шлюз (gateway), ориентированные на функции информационной защиты сетей. Такая структура межсетевых соединений позволяет резко снизить угрозу несанкционированного доступа в локальную и распределенную сеть за счет использования способа маскарада (masquerading), когда весь исходящий из РС трафик посылается от имени СЗИ, делая РС практически «невидимой». Методы передачи информации в таких сетях рассматриваются в [2-4].

Анализ показывает, что перечисление возможных угроз сети практически невыполнимо из-за огромного их количества. Поэтому на основе некоторых характерных особенностей, таких как запрограммированные или незапрограммированные действия, засорение почтового ящика, нахождение черных ходов, загромождение канала, выведение из строя компьютера и т.д. в [1] предлагается классификация возможных угроз сети, как троянский конь (ТК), вирусы (В), сообщение засоряющие почтовый ящик (СЗПЯ), черные ходы (ЧХ), атаки нацеленные на отказ сервиса (АНОС) и некорректно работающие программы (НРП).

Задача определения характеристик систем защиты информации (СЗИ) в РС решается на основе приведенной классификации возможных угроз сети. Исходя из практических соображений можно принять, что число злоумышленных программ (сообщений) составляет треть от общего числа сообщений.

Распределенные сети, функционирующие в условиях большой интенсивности при пуассоновском потоке с групповым поступлением, рассмотрены в [5] . Другие модели, связанные с развитием методов маршрутизации и управления потоком, анализируются в [6]. В целях обеспечения информационной безопасности сетей необходимо организовать некоторую систему защиты, включающие современные технические средства[7] для контроля передаваемой информации и их комплексной защиты от различных воздействий. Эти системы содержать некоторый комплекс программ, требующий определенный объем памяти:

- программы, осуществляющие криптографические шифрование почтовых сообщений, таких как Pretty Good Privacy (PGP);
- утилиты, позволяющие обнаруживать и уничтожать «шпионские» программы , например Ad – aware X cleaner;
- брандмауэры, обнаруживающие и блокирующие несанкционированный доступ к компьютеру, не допускающие попадания на жесткий диск «мусора», «шпионского» программного обеспечения и «троянов»;
- антивирусные программы (Antivral Toolkit, Kaspresky antivirius, Dr.Web и др.) и различные утилиты, направленные на борьбу с конкретными вирусами.

Проведение периодического анализа эффективности СЗИ является одной из основных задач в РС [7]. Путем совершенствования и оптимизации характеристик систем защиты можно обеспечить достаточно высокую их эффективность, труднопреодолимую даже опытному злоумышленнику. Решение этих проблем требуют разработки соответствующих математических моделей и метод их анализа.

В доступной литературе известны некоторые попытки решения указанных проблем [2-4]. Они в основном используют методы защиты информации на уровне имени и пароля пользователя, которые недостаточна для предотвращения входа в сеть посторонних лиц. Кроме того большое число потенциальных каналов проникновения в сеть еще больше усложняет защиту информации в сети. В отличие от указанных работ здесь предложен альтернативный подход к решению задачи по определению оптимальной программно-технической структуры СЗИ. Этот подход основан на принципах теории

систем массового обслуживания (СМО), учитывающих характеристики воздействя возможных угроз на функционирование сети.

Целью данного исследования является сравнительный анализ результатов математических и имитационных моделей систем защиты информации в распределенных сетях обслуживания.

Постановка задачи

Проблема состоит в разработке эффективного подхода к решению задачи сравнительного анализа результатов расчета и оптимизации функциональной структуры системы защиты информации в РС. В качестве математической модели СЗИ может служить следующая многоканальная СМО, состоящая из N компьютеров. Компьютеры характеризуются, в основном, интенсивностями обслуживания, распределенные по экспоненциальному закону, при этом на вход системы поступает пуассоновский поток сообщений с интенсивностью λ_P, время обслуживания подчиняется экспоненциального, постоянного и эрлангового закона распределения. Поступающая информация фильтруется и распределяется по сети.

Функционирование сети может быть нарушено со стороны злоумышленников и восстанавливаться с помощью комплекса программ, как во время передачи сообщений, так и в промежутке времени, когда передача сообщений не производится. Предполагается, что время передачи информации (T_{ci}), время исправной работы сети ($T_i = 1/d_i$), время ее восстановления (T_{ni}) и время старения информации ($T_D = 1/\nu$) в условиях возможных угроз со стороны злоумышленников распределены по экспоненциальному закону с параметрами μ_i, c_i, d_i, ν соответственно.

Показателем эффективности является математическое ожидание вероятности потери от несвоевременного распределения сообщений после фильтрации по компьютерам сети, т.е. требуется решить следующую задачу [1]:

$$M\left[\bar{P}\right] = \min \sum_{i=1}^{N} p_i q_i \tag{1}$$

при ограничениях

$$1 - \sum_{i=1}^{N} p_i = 0, \quad 0 \le P_i \le \mu_i k_i / \lambda, \quad i = \overline{1, N}, \tag{2}$$

$$\text{где } \mu_i = 1/T_{ci},\ h(p) = 1 - \sum_{i=1}^{N} p_i,\ q_i(p) = p_i,\ q_2(p) = p_i \le \frac{\mu_i k_i}{\lambda}, \tag{3}$$

$$q_i = \frac{(1 - p_i \lambda h_{1i})}{(1 - p_i \lambda h_{1i} + \nu_i h_{1i}}, \ h_{1i} = \frac{1}{\mu_i k_i}, \ \nu_i = \nu\left[k_i + \frac{(1-k_i)(\nu - p_i\lambda)}{\nu(1+\nu T_{ni}}\right], \ i = \overline{1, N}. \tag{4}$$

Здесь приняты следующие обозначения: $\bar{P}$ - вероятность потери от несвоевременного распределения сообщений по компьютерам после фильтрации в РС, p_i - вероятность потери от непопадания сообщений для передачи на i-й компьютер, q_i - вероятность потери в i-м компьютере от несвоевременной доставки сообщений, k_i - коэффициент готовности, T_{ni} - среднее время простоя.

Для решения задачи (1)-(4) в [1] предлагается использовать метод обобщенного приведенного градиента [8], на основе который разработаны алгоритмы расчета и оптимизации характеристик СЗИ относительно выбранного критерия качества. Этот метод позволяет исследовать поведение СЗИ при любых диапазонах изменения структурных и нагрузочных параметров модели.

Анализ результатов математической модели СЗИ в РС

С целью расчета характеристик СЗИ на основе разработанного алгоритма проведены объемные вычислительные эксперименты в широких диапазонах изменения как структурных, так и нагрузочных параметров модели. Так, для исходных данных $1/\mu_i = (0.042; 0.042; 0.063)$, $k_i = (0.97; 0.79; 0.81)$, $T_{n_i} = (0.6; 0.9; 1.0)$, $\nu = 0.5 (T_D = 2)$ исследованы зависимости $p_i = f(\lambda), i = \overline{1,3}$. Соответствующие результаты показанны в табл.1.

Таблица 1. Зависимости $p_i = f(\lambda), i = \overline{1,3}$.

λ	p_1	p_2	p_3
1/1000	1.00	0	0
1/2000	0.80	0.20	0
1/3000	0.78	0.22	0
1/4000	0.76	0.24	0
1/5000	0.71	0.29	0
1/6000	0.73	0.27	0
1/7000	0.69	0.21	0.10
1/8000	0.65	0.23	0.12
1/9000	0.62	0.25	0.13
1/10000	0.59	0.27	0.14
1/11000	0.56	0.29	0.15

В силу допустимых потерь информации полученные в табл.1, определены основные характеристики многоканальной СМО для экспоненциального, постоянного и Эрлангового времени обслуживания. Здесь основные характеристики являются L_q - длина очереди, L_s - количество сообщений в системе, τ_q - время ожидания сообщений в очереди, τ_s - время пребывания сообщений в системе (см. табл.2-4)..

Таблица 2. Результаты для экспоненциального времени обслуживания

$a = \lambda / \mu N$	L_q	L_s	τ_q	τ_s
0.95	7.75	8.23	10856	13210
0.67	0.53	2.34	795	3497
0.46	0.14	1.92	172	2708

Таблица 3. Результаты для постоянного времени обслуживания

$a = \lambda / \mu N$	L_q	L_s	τ_q	τ_s
0.95	1.138	2.69	1998	3805
0.67	0.46	2.30	547	3057
0.46	0.087	1.82	117	2642

Таблица 4. Результаты для Эрлангового времени обслуживания

$a = \lambda / \mu N$	L_q	L_s	τ_q	τ_s
0.95	3.72	4.21	3850	7250
0.67	0.63	2.74	352	1497
0.46	0.17	1.35	94	1308

Эти результаты подтвердили теоретические ожидания относительно поведения функции потери от несвоевременного распределения сообщений по компьютерам после фильтрации в РС, с определенной схемой маршрута распределения сообщений в сети в условиях возможных угроз со стороны злоумышленников.

При построении СЗИ в РС, наряду с аналитическими методами моделирования зачастую используют и метод имитационного моделирования [9]. Последний метод представляет разработчикам возможность исследования объектов практически любой сложности. При этом имитационное моделирование используется как составная часть системы автоматизации проектирования на этапах эскизного и технического проектирования. К числу наиболее широко распространенных инструментальных средств, обеспечивающих поддержку принятия решения, относится General Purpose Simulation System (GPSS) [9].

Анализ результатов имитационной модели СЗИ в РС

Рассматриваются варианты имитационных моделей СЗИ в РС, имеющие следующие схемы маршрутизации сообщений двух типов. Маршрут обработки сообщений для первого типа выполняется по функциям (операции по защиты информации) 1-3, а для сообщений второго типа выполняется по функциям (операции по защиты информации) 4-6. Распределение выполняемые функции защиты информации по компьютерам $k_i, i = \overline{1,3}$ приведены в табл.5. Интервалы времени между поступающими сообщениями и времена их выполнения приведены в табл.6 и 7.

Таблица 5. Распределение функции защиты информации по компьютерам $k_i, i = \overline{1,3}$

Функции	Функция 1	Функция 2	Функция 3	Функция 4	Функция 5	Функция 6
варианты	k_1	k_2	k_3	k_1	k_2	k_3
1	k_1	k_2	k_3	k_3	k_2	k_1
2	k_1	k_2	k_3	k_3	k_1	k_2
3	k_1	k_2	k_3	k_1	k_2	k_3
4	k_1	k_2	k_3	k_2	k_1	k_3
5	k_1	k_2	k_3	k_2	k_3	k_1
6	k_2	k_1	k_3	k_1	k_2	k_3
7	k_2	k_1	k_3	k_1	k_3	k_2
8	k_2	k_1	k_3	k_2	k_1	k_3
9	k_2	k_1	k_3	k_2	k_3	k_1
10	k_2	k_1	k_3	k_3	k_1	k_2
11	k_2	k_1	k_3	k_3	k_2	k_1
12	k_3	k_1	k_3	k_1	k_2	k_3

Требуется определить среднюю загрузку каждого компьютера, среднее время обработки сообщений каждого типа, длина очередей на обработку для компьютеров, объем памяти, необходимый для данного потока сообщений. В модели таймер настроен на выполнение моделирования в течение установленного модельного времени. При необходимости таймер должен быть откорректирован. После прогона модели имитации СЗИ в РС получены результаты, которые показаны в табл.8-10.

Таблица 6. Интервалы времени поступления сообщений

Вариант	Интервал времени поступления сообщений первого типа	Интервал времени поступления сообщений второго типа
	30 ± 5	20 ± 5
1	25 ± 4	25 ± 6
2	20 ± 3	30 ± 7
3	15 ± 5	35 ± 8
4	10 ± 4	20 ± 5
5	30 ± 5	10 ± 3
6	15 ± 4	15 ± 6
7	30 ± 10	15 ± 3
8	20 ± 5	20 ± 5
9	25 ± 4	10 ± 3
10	45 ± 5	15 ± 5
11	20 ± 4	15 ± 3
12	10 ± 3	15 ± 5

Таблица 7. Интервалы времени выполнения функции защиты информации (мин)

Вариант	1	2	3	4	5	6
	5 ± 2	2 ± 4	10 ± 3	7 ± 3	15 ± 5	15 ± 5
1	20 ± 4	5 ± 2	15 ± 5	15 ± 5	7 ± 3	10 ± 3
2	10 ± 3	15 ± 3	5 ± 2	20 ± 4	10 ± 3	7 ± 3
3	18 ± 3	10 ± 3	12 ± 5	20 ± 4	25 ± 8	12 ± 4
4	12 ± 5	15 ± 5	18 ± 3	10 ± 3	5 ± 2	20 ± 4
5	15 ± 5	20 ± 4	10 ± 3	18 ± 3	12 ± 5	2 ± 4
6	10 ± 3	25 ± 8	5 ± 2	14 ± 5	18 ± 3	15 ± 5
7	15 ± 5	12 ± 5	20 ± 4	5 ± 2	10 ± 3	18 ± 3
8	20 ± 4	18 ± 3	10 ± 3	7 ± 3	15 ± 5	25 ± 8
9	10 ± 3	15 ± 5	10 ± 3	12 ± 5	5 ± 2	20 ± 4
10	25 ± 8	5 ± 2	12 ± 5	7 ± 3	10 ± 3	15 ± 5
11	20 ± 4	10 ± 3	15 ± 5	5 ± 2	12 ± 5	25 ± 8
12	12 ± 5	20 ± 4	25 ± 8	15 ± 5	5 ± 2	10 ± 3

Таблица 8. Средняя загрузка компьютеров (в %)

компьютер	в течение 8ч.	в течение недели
k_1	48	52
k_2	92	98
k_3	88	96

Таблица 9. Максимальная длина очередей к компьютерам

компьютер	в течение 8ч.	в течение недели
k_1	1	1
k_2	12	59
k_3	2	3

Таблица 10. Среднее время обработки сообщений на компьютерах (в мин.)

компьютер	в течение 8ч.	в течение недели
k_1	5.9	6.31
k_2	16.33	16.99
k_3	12.38	13.18

По результатам моделирования можно сделать вывод о том, что общее число обработанных сообщений в течение 8 часов составляет 40, в в течение рабочей недели составляет 142. Эти данные позволяют рассчитывать необходимого объема памяти для СЗИ в РС. При этом первый компьютер k_1 загружен на 50% и перегружен компьютер k_2 (об этом говорит средний процент использования 98% и длина очереди 59). При этом компьютер k_3 загружен оптимально. Отметим, что для повышения эффективности функционирования СЗИ в РС при данном потоке сообщений можно использовать два компьютера.

С целью определения оптимальной структуры СЗИ в РС при заданном потоке сообщений можно продолжить прогона модели. Кроме того, если структуру сети менять нельзя, то используя возможности языка моделирования GPSS можно подобрать такой поток сообщений, который позволил бы возможность загружать сети оптимально.

Разработка алгоритма анализа и сравнение результатов

математических и имитационных методов

С целью сравнительного анализа результатов математических и имитационных методов разработан алгоритм, который имеет следующие шаги.

Шаг 1. Построение модели имитации для различных случаев.

Шаг 2. Выполнение процесса имитации при нормальных условиях, получение различных вариантов и обоснование модели.

Шаг 3. Сравнение результатов математических и имитационных моделей.

Шаг 4. Если результаты математических и имитационных моделей сходятся, выполняются имитации для пиковой нагрузки. В противном случае система расширяет свои возможности (т.е. увеличивается значения структурных параметров).

Шаг 5. Осуществляется процесс тестирования (построение и обработка РС и проверка всех функций).

Шаг 6. Выполнение имитации при нормальных условиях и построение для получения различных вариантов.

Шаг 7. Проверка сходимости результатов. Если они сходятся, сеть проверятся дополнительно в условиях пиковых нагрузок. В противном случае сеть расширяет свою возможность и осуществляется переход к четвертому шагу.

Сравнения результатов математических и имитационных моделей осуществляется так:

$$\Delta P = \left[\frac{(P^{\bullet} - P)}{P} \right].100\,\%$$

где $P^{\bullet}$, P – значения характеристик математических и имитационных моделей, соответственно.

На основе разработанного алгоритма анализ результатов полученных после прогона обоих модели показывает, что они отличаются в пределах 2-10%, а степень адекватности математической модели к исследуемому объекту увеличивается с уменьшением значения нагрузки $a = \lambda / \mu N$.

Выводы и рекомендации

Проведен сравнительный анализ результатов математических и имитационных моделей системы защиты информации в распределенных компьютерных сетях. Проведены вычислительные эксперименты на основе разработанных алгоритмов и получены численные результаты, которые могут быть использованы при построении СЗИ в РС производственного назначения.

Анализ результатов обоих модели показывает, что они отличаются в пределах 2-10%, а степень адекватности математической модели к исследуемому объекту увеличивается с уменьшением нагрузки $a = \lambda / \mu N$.

Список литературы

1. Исмайлов Б.Г. Исследование характеристик систем защиты информации распределенной сети // Автоматика и вычислительная техника. Рига.: 2006, №3. с.51-59, {ISSN 0132-4160}.
2. Герасименко В.А., Малюк А.А. Основы защиты информации. М.: ППО «Известия» УДПРФ. 1997. 372 с., {ISSN 002-2197}.
3. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. Развитие, итоги, перспективы // Зарубежная радиоэлектроника, 1993, №3, с.3-21.{ISSN3.3-14/111-93}.
4. Грушо А.А., Тимонина Е.Е. Теоретические основы защита информации. М.: Издательство Агентства «Яхтсмен», 1996. 130с. {ISBN 11-96}
5. Алиев А.А., Исмайлов Б.Г. Анализ характеристик многопотоковых сетей обслуживания // Радиоэлектроника, информатика и управление, Запорожье.: 2001, №2. с.66-69 {ISSN 01886}
6. N.F. Maxchemchuk, ,M.Ei.Zarki. Routing and flow control in high–speed wide area networks // Proc. of the IEEE. 1990, Vol. 78, N1. p. .204-221. {ISBN 01890}.
7. Алябев С.В. Проблемы защиты информации в сети промышленного предприятия // Сб.трудов ПУКИ, Выпуск 8 (Воронеж).Центральное Черноземное книжное издательство, 2003. с.69-70. {ISBN 5.7458-0575-7}.
8. Химмелблау Д. Прикладное нелинейное программирование.- М.: Мир,1975.,540с. {ISBN 01/75}.
9. Шрайбер Т.Дж. Моделирование на GPSS.- М.: Машиностроение,1980,-592с. {ISSN 02880}.

Сведения об авторах

Исмайлов Балами Гасым оглы, доцент кафедры Информатики Сумгаитского Госдарственного Университета, гор. Сумгаит 43-й квартал. Email: Balemi@rambler.ru