УДК 681.324

Б. Г. Исмайлов, к. т. н., доц.

АНАЛИЗ РЕЗУЛЬТАТОВ МОДЕЛИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В РАСПРЕДЕЛЕННЫХ СЕТЯХ ОБСЛУЖИВАНИЯ

В статье проведен 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.

Ключевые слова: *система защиты информации, распределенные сети обслуживания, моделирование.*

Введение

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 проходящую через них информацию. Это своего рода межсетевой шлюз (gateway), ориентированный на функции информационной защиты сетей. Такая структура межсетевых соединений позволяет резко снизить угрозу несанкционированного доступа в локальную и распределенную сети за счет использования способа маскирования (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].

Проведенный анализ показывает, что перечисление возможных угроз сети практически невыполнимо из-за их большого 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. Классификация включает такие угрозы как: троянский конь (ТК), вирусы (В), сообщения, засорявшие почтовый ящик (СЗПЯ), черные ходы (ЧХ), атаки, нацеленные на отказ сервиса (АНОС), и некорректно работающие программы (НРП).

Задача определения характеристик 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 систему защиты, включающую современные технические средства [7] для контроля передаваемой информации и их комплексной защиты от различных воздействий. Эти системы содержат комплекс программ, требующий определенного объема памяти:

– программы, осуществляющие криптографическое шифрование почтовых сообщений, такие 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 описанных выше проблем требует разработки соответствующих математических моделей и методов их анализа.

В доступной литературе известны попытки решения указанных проблем [2 – 4]. Они в основном используют методы защиты информации на уровне имени и пароля пользователя, которые недостаточны 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 в статье 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 воздействий возможных угроз на функционирования сети.

Цель исследования

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, распределенными по экспоненциальному закону, при этом на вход системы поступает пуассоновский поток сообщений с интенсивностью λ_P, время обслуживания подчиняется экспоненциальному, постоянному и эрланговому законам 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]:

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

при ограничениях

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

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

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

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

С целью решения задачи (1) – (4) в [1] предлагается использовать метод обобщенного приведенного градиента [8], на основе которого разработаны алгоритмы расчета и оптимизации характеристик СЗИ по выбранному критерию качества. Этот метод позволяет исследовать поведение СЗИ при любых диапазонах изменения структурных и нагрузочных параметров модели.

Анализ результатов математической модели СЗИ в РС

Для расчета характеристик СЗИ на основе разработанного алгоритма проведены многочисленные вычислительные эксперименты в широких диапазонах изменения как структурных, так и нагрузочных параметров модели. Так, для исходных данных $1/\mu_i = (0{,}042;0{,}042;0{,}063)$, $k_i = (0{,}97;0{,}79;0{,}81)$, $T_n = (0{,}6;0{,}9;1{,}0)$, $\nu = 0{,}5 (T_D = 2)$ исследованы зависимости $p_i = f(\lambda), i = \overline{1,3}$. Соответствующие результаты показаны на рис. 1.

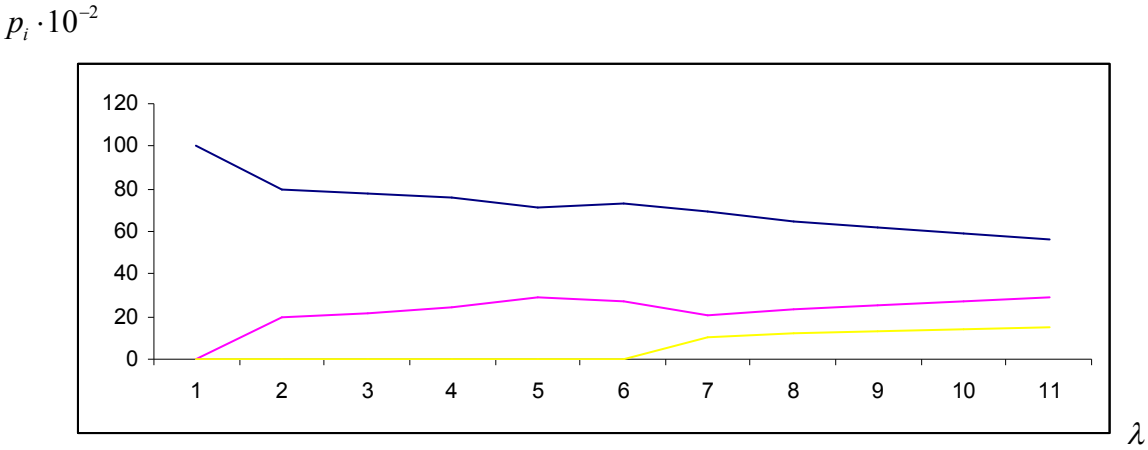


Рис. 1. Зависимости $p_i = f(\lambda), i = \overline{1,3}$

В силу допустимых потерь информации, показанных на рис. 1, определены основные характеристики многоканальной СМО для экспоненциального, постоянного и эрлангового времени обслуживания. Здесь основными характеристиками 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 (рис. 2 – 7, $a = (0{,}95;0{,}67;0{,}46)$, L_q, τ_q – верхняя линия, L_s, τ_s – нижняя линия).

$L_q 10^{-2},\ L_s 10^{-2}$

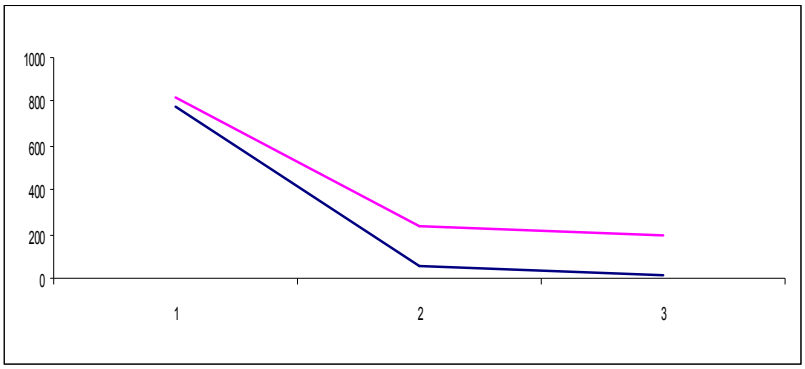


Рис 2. Зависимости $L_q = f(a),\ L_s = f(a)$ для экспоненциального времени обслуживания $\tau_q,\ \tau_s$

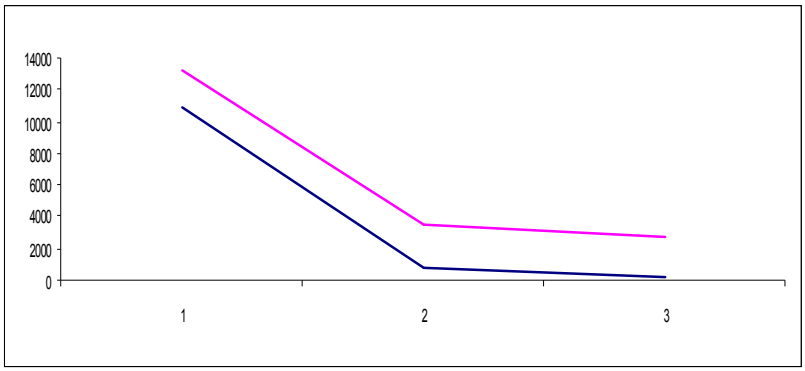


Рис 3. Зависимости $\tau_q = f(a),\ \tau_s = f(a)$ для экспоненциального времени обслуживания $L_q 10^{-2},\ L_s 10^{-2}$

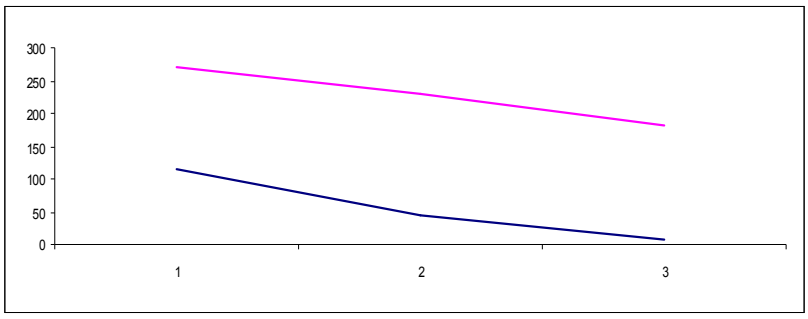
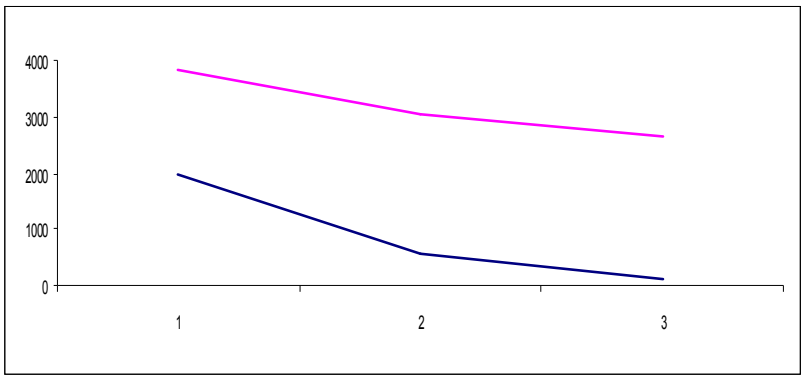


Рис 4. Зависимости $L_q = f(a),\ L_s = f(a)$ для постоянного времени обслуживания

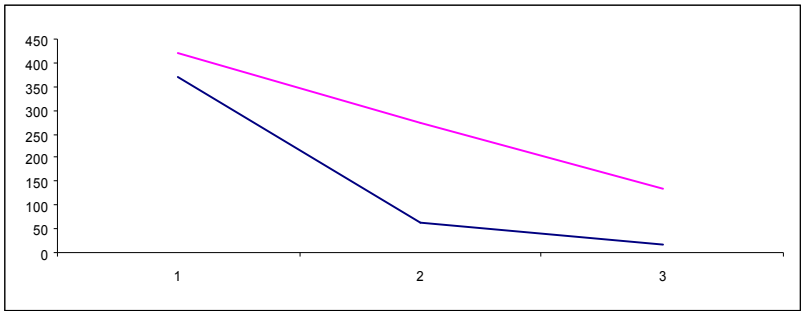
$\tau_q,\ \tau_s$



$a = \lambda / \mu N$

Рис 5. Зависимости $\tau_q = f(a)$, $\tau_s = f(a)$ для постоянного времени обслуживания

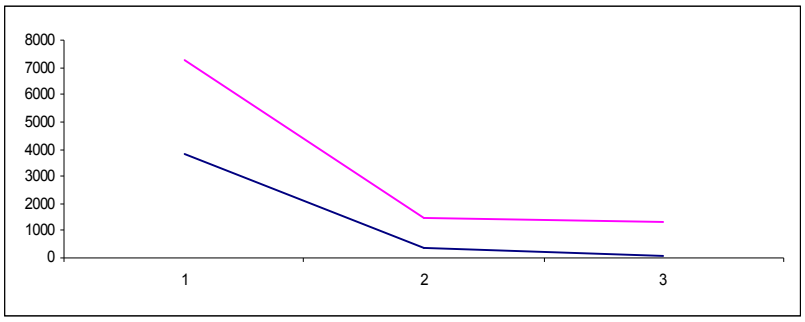
$L_q 10^{-2},\ L_s 10^{-2}$



$a = \lambda / \mu N$

Рис 6. Зависимости $L_q = f(a)$, $L_s = f(a)$ для эрлангового времени обслуживания

$\tau_q,\ \tau_s$



$a = \lambda / \mu N$

Рис 7. Зависимости $\tau_q = f(a)$, $\tau_s = f(a)$ для эрлангового времени обслуживания

Полученные 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]. Этот 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 защите информации) [1 – 3], а для сообщений второго типа выполняется по функциям (операции по защите информации) [4 – 6]. Распределение выполняемых функций защиты информации по компьютерам $k_i, i = \overline{1,3}$, интервалы времени между поступающими сообщениями и время их выполнения заданы.

Требуется определить среднюю загрузку каждого компьютера, среднее время обработки сообщений каждого типа, длину очередей на обработку для компьютеров, объем памяти, необходимый для данного потока сообщений. В модели таймер настроен на выполнение моделирования в течении установленного модельного времени. При необходимости таймер должен быть откорректирован. После прогона модели имитации СЗИ в РС получены результаты. На основе этих результатов построены и исследованы зависимости, которые показаны на рис. 8 – 10.

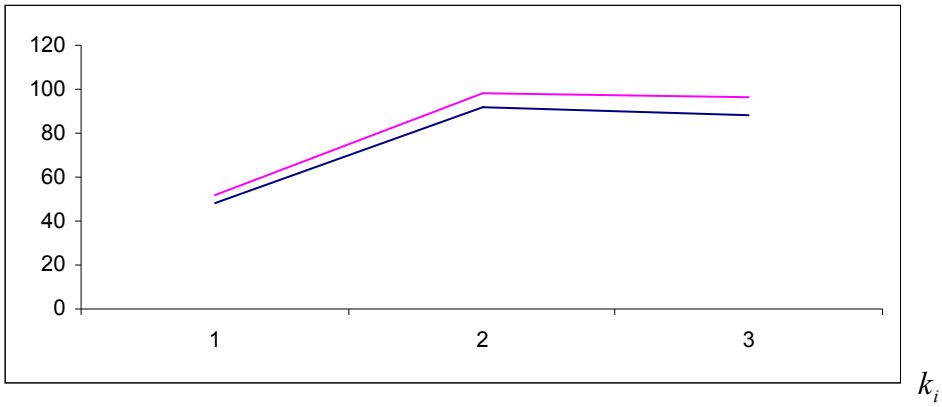


Рис 8. Средняя загрузка компьютеров (в %) k_i, в течении 8 ч. (верхняя линия), в течении недели (нижняя линия)

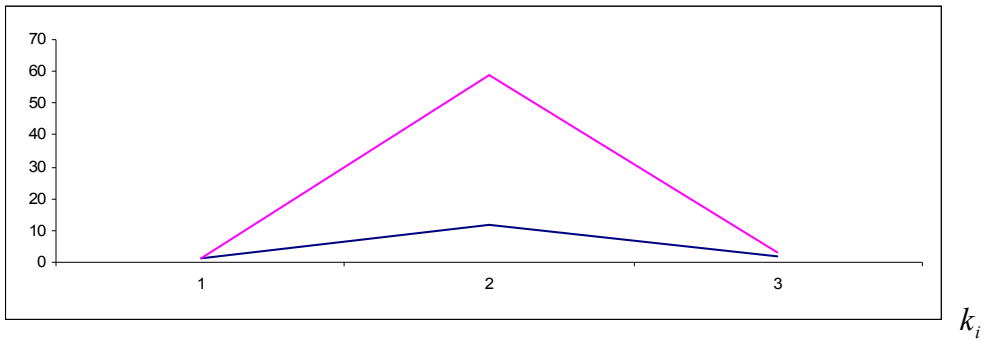


Рис 9. Максимальная длина очередей к компьютерам k_i, в течении 8 ч. (верхняя линия), в течении недели (нижняя линия)

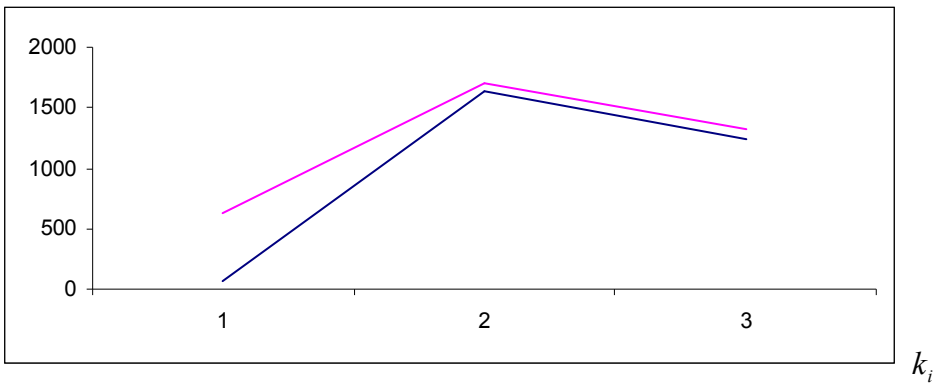


Рис 10. Среднее время обработки сообщений на компьютерах (в мин.) k_i, в течении 8 ч. (верхняя линия), в течении недели (нижняя линия)

По результатам моделирования можно сделать вывод о том, что общее число обработанных сообщений в течении 8 часов составляет 40, в течении рабочей недели – 142. Эти данные позволяют рассчитывать необходимый объем 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 сообщений). 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 прогон модели. Кроме того, если структуру сети менять нельзя, то, используя возможности языка моделирования GPSS, можно подобрать такой поток сообщений, который позволил бы 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 проверяется дополнительно в условиях пиковых нагрузок. В противном случае сеть расширяет свои возможности и осуществляется переход к четвертому шагу.

Сравнения результатов математических и имитационных моделей осуществляется так:

$$\Delta P = \left[\frac{(P^{\bullet} - P)}{P} \right] \cdot 100\%, \qquad (5)$$

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

На основе разработанного алгоритма анализ результатов, полученных после прогона

обоих моделей, 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

Проведен сравнительный анализ результатов математических и имитационных моделей системы защиты информации в распределенных компьютерных сетях. Осуществлены вычислительные эксперименты на основе разработанных алгоритмов и получены численные результаты. Анализ результатов обоих моделей 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 / Б. Г. Исмайлов // Автоматика и вычислительная техника. – Рига: – 2006. – №3. – С. 51 – 59.

2. Герасименко В. А. Основы защиты информации / В. А. Герасименко, А. А. Малюк. – М.: ППО «Известия» УДПРФ. – 1997. – 372 с.

3. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. Развитие, итоги, перспективы / В. А. Герасименко // Зарубежная радиоэлектроника. – 1993. – № 3. – С. 3 – 21.

4. Грушо А. А. Теоретические основы защиты информации / А. А. Грушо, Е. Е. Тимонина. – М.: Издательство Агентства «Яхтсмен». – 1996. – 130 с.

5. Алиев А. А. Анализ характеристик многопотоковых сетей обслуживания / А. А. Алиев, Б. Г. Исмайлов // Радиоэлектроника, информатика и управление. – Запорожье: 2001. – № 2. с. 66 – 69.

6. Maxchemchuk N. F. Routing and flow control in high–speed wide area networks / N. F. Maxchemchuk, M. Ei. Zarki // Proc. of the IEEE. – 1990. – Vol. 78. – N1. – P. 204 – 221.

7. Алябев С. В. Проблемы защиты информации в сети промышленного предприятия / С. В. Алябев // Сб. трудов ПУКИ. – 2003. – Выпуск 8. Воронеж: Центральное Черноземное книжное издательство. – С. 69 – 70.

8. Химмелблау Д. Прикладное нелинейное программирование / Д. Химмелблау. – М.: Мир, 1975. – 540 с.

9. Шрайбер Т. Дж. Моделирование на GPSS / Т. Дж. Шрайбер – М.: Машиностроение, 1980. – 592 с.

Исмайлов Балами Гасым оглы – доцент кафедры информатики. Email: Balemi@ rambler.ru
Сумгаитский государственный университет.