УДК 519.872

АНАЛИЗ СИСТЕМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ С ОГРАНИЧЕННЫМИ БУФЕРАМИ В СЕТЯХ ОБСЛУЖИВАНИЯ

Исмайлов Балами

Национальная Академия Авиации, AZ1045 Баку, Азербайджан

Аннотация

Рассмотрены системы безопасности информации (СБИ) с ограниченными буферами, обеспечивающие максимальную информационную безопасность сетей обслуживания путем обеспечения перехода всех запросов несанкционированного доступа (НСД) от механизма защиты (МЗ).

Разработаны модели и алгоритмы исследования оптимальных характеристик СБИ как однофазных многоканальных систем массового обслуживания (СМО) с ограниченным временем ожидания. Проведены вычислительные эксперименты и получены численные результаты, которые позволяют использовать их при построении СБИ в сетях различного назначения.

Abstract

Information security systems (ISS) with limited buffers are considered, which ensure the maximum information security of service networks by ensuring the transition of all unauthorized access requests (UAR) from the protection mechanism (PM).

Models and algorithms for studying the optimal characteristics of ISS as single-phase multichannel queuing systems (QS) with a limited waiting time are developed. Computational experiments were carried out and numerical results were obtained that allow them to be used in the construction of ISS in networks for various purposes.

Введение

В настоящее время развитие научного направления в области оценки защищенности информации в сетях обслуживания с использованием систем безопасности информации, осложняется отсутствием единой методики для оценки СБИ. Эффективность безопасности информации в сетях обслуживания определяется, в основном, классом защищенности сети обслуживания, который определяет набор механизмов защиты (МЗ) реализованных в сети.

В работах [1-3] предлагаются методы и методики, позволяющие выполнять количест-венную оценку защищенности информации при использовании СБИ, которые проводятся определенным набором вероятностных показателей. Для обоснования методики оценки защищенности информации в [1] разработана теоретическая модель СБИ от НСД, при которой исходный поток НСД разрежается с определенными вероятностями и образует выходной поток. В работах [1,2] отмечается, что существует факт неполного закрытия системой защиты всех возможных каналов проявления угроз, т.е. не для всех входных потоков достается МЗ. В результате запросы НСД не проходят проверки средств защиты и пропускаются к защищаемому ресурсу, что в итоге реализует соответствующую угро-зу. Поэтому возникает задача определения оптимальной конфигурации СБИ, обеспечи-вающей максимальную информационную безопасность сетей обслуживания путем обес-печения перехода всех запросов НСД от МЗ. В отличие от [1,2] с целью полного закры-тия системой защиты всех возможных каналов в работе предлагается структура СБИ с ограниченным буфером. При этом преследуется цель разработки математической модели СБИ, позволяющей в силу имеющихся ограниченных ресурсов определить оптимальные характеристики системы.

В структуре нарушитель (злоумышленник), т.е. запросы НСД на входе системы, создает разные угрозы информации с интенсивностью λ. СБИ от НСД представляет

собой аппаратно-программный комплекс, взаимодействующий с потоками случайных событий. Они обуславливаются рядом причин как действиями злоумышленников, неправильным распределением прав доступа, использованием несанкционированного программного обеспечения, ошибками в программно-технических комплексах идентификации, аутентификации и т.д. СБИ состоит из общего ограниченного буфера для ожидания в очереди запросов НСД за некоторое время τ_q, которые осуществляют задержки $\tau_0 = 1/\mu$ на обслуживание, где μ - интенсивность обслуживания запросов НСД и N - количество МЗ. При обслуживании происходит отсеивание запросов НСД. В СБИ со стороны МЗ выполняется обнаружение и классификация попыток НСД и при необходимости с определенными вероятностями исполняются функции блокирования или пропуска запросов НСД к защищаемым ресурсам. Пропущенные (нераспознанные) запросы могут нанести вред защищаемым ресурсам. Защищаемые ресурсы не выполняют самостоятельных функций.

Целью данной работы является поиск оптимальных конфигураций СБИ, позволяющих функционировать при ограниченных ресурсах. Предполагается, что входной поток информации, т.е. запросы НСД, являются простейшими, а время обслуживания подчиняется экспоненциальному, постоянному и Эрланговому закону распределения. Если рассматривать блок нарушителя как источник информации, а МЗ как параллельно работающие приборы, то СБИ можно рассматривать как однофазную многоканальную систему массового обслуживания с ограниченным временем ожидания. При этом требуется определить оптимальные характеристики таких систем: длину очереди определяющей объем памяти (буфера), количество параллельно работающих приборов обслуживания (МЗ), количество запросов в системе, время ожидания запросов в очереди и время пребывания запросов в системе в пределах допустимых потерь запросов.

Показателем эффективности такой системы может быть минимизация математического ожидания вероятности потери запросов НСД из-за перегрузки системы обслуживания.

$$M\,[\mathrm{P}(\lambda,\mu,\mathrm{N})] \to \min$$

при $\lambda \ge \lambda_0, \mu \ge \mu_0, N \ge N_0,$

$L_q \le L^0$

где M - знак математического ожидания, $\mathrm{P}(\lambda,\mu,\mathrm{N})$ - вероятность потери запросов НСД из-за перегрузки системы, L_q - длина очереди, т.е. величина определяющая объем буферной памяти СБИ, $\lambda_0, \mu_0, N_0, L^0$ - допустимые предельные значения.

Разработаны математическая модель и алгоритм для исследования СБИ как однофазных многолинейных СМО с ограниченной буферной памятью. Алгоритм получения оптимальных значений характеристик системы включает следующие шаги:

- На первом шаге после ввода значений L^0, средних значений λ, μ и установления начального значения $N = N^0$ определяются потери запросов. На последующих шагах это соотношение нормализуется для трех случаев аналитического анализа характеристик.

1. Интенсивность поступления и время обслуживания (ВО) запросов подчиняются экспоненциальному закону. При удовлетворении условия $L_q \le L^0$ процесс считается нормальным, поэтому полученные характеристики выводятся и аналитический анализ завершается. В противном случае анализ продолжается и осуществляется переход ко второму шагу.

2. Интенсивность поступления запросов подчиняется экспоненциальному закону, а обслуживание - постоянному (детерминированному). При неудовлетворении условия $L_q \le L^0$ система должна расширить свои возможности путём $N = N + 1$, а при удовлетворении - осуществить переход к шагу три.

3. Выполнение условий нормальности по постоянному закону обслуживания может оказаться недостаточным для учета некоторых других требований к системе, например, надёжности. Поэтому аналитический анализ характеристик системы проводится дополнительно для Эрлангового закона распределения. Выполнение условия $L_q \le L^0$ является достаточным для завершения анализа. При невыполнении данного условия осуществляется переход к первому шагу алгоритма путем $N = N + 1$.

Проведены вычислительные эксперименты и получены численные результаты. С целью проверки адекватности полученных результатов, а также подробного анализа характеристик СБИ при экспоненциальных входных, экспоненциальных, постоянных и Эрланговых выходных потоков для их различных значений и с учетом их трудоемкости, разработаны имитационные модели изучаемых систем на языке GPSS.

В модели рассматривается однофазная многоканальная система, в которую на обслуживание поступает пуассоновские входные потоки, а время обслуживания транзактов, соответственно, подчиняются экспоненциальному, постоянному и Эрланговому законы распределения. В модели транзакты образуют ограниченную очередь в буферной памяти.

Проведены имитационные эксперименты и получены результаты. Сравнительный анализ результатов аналитический модели с результатами модели имитации показывает, что они хорошо согласованы, а полученные результаты могут быть использованы при построены СБИ в сетях различного назначения.

Список использованных источников

1. Карпова В.В. Вероятностная модель оценки защищенности средств вычислительной техники с аппаратно-программным комплексом защиты информации от несанкционированного доступа//Программные продукты и системы № 1, 2003,с.31-36.

2. Григорьев В.А., Карпова А.В. Имитационная модель системы защиты информации //Программные продукты и системы № 2, 2005,с.26-30.

3. Карпова А.В. Оценка защищенности информации от несанкционированного доступа при помощи имитационной модели системы защиты информации //Программные продукты и системы № 2, 2005,с.51-54.