DOI: 10.25728/avtprom.2020.07.05

Моделирование системы безопасности информации в сетях обслуживания объектов нефтегазодобычи

Б.Г. Исмайлов (Национальная Академия Авиации Азербайджана)

Решается задача выбора оптимальной конфигурации системы безопасности информации (СБИ), обеспечивающей максимальную информационную безопасность сетей обслуживания объектов нефтегазодобычи путем распознавания всех запросов несанкционированного доступа (НСД) механизмами защиты (МЗ). Разработаны вычислительные процедуры и алгоритмы исследования оптимальных характеристик СБИ как однофазных многоканальных систем массового обслуживания (СМО) с потерями. Проведены вычислительные эксперименты и получены численные результаты, которые позволяют использовать предложенный подход при построении СБИ в сетях различного назначения.

Ключевые слова: системы безопасности информации, системы с потерями, механизм защиты, несанкционированный доступ, системы массового обслуживания, время обслуживания.

Введение

Настоящая статья является продолжением рассматриваемых проблем, характерных для систем с потерями, с ограниченными и неограниченными объемами буферной памяти [1]. Исследуются модели, в которых структура системы безопасности базируется на системах безопасности информации (СБИ) без буферной памяти.

Отметим, что в настоящее время значимость проблемы информационной безопасности является признанной, и подтверждением этого являются огромные убытки, понесенные корпорациями из-за недостаточной защищенности информации [2, 3, 4].

Проведенный анализ и накопленный опыт в области информационной безопасности и разработки СБИ указывают на наличие серьезных трудностей, которые во многом связаны с отсутствием единой системы оценки защищенности информации, позволяющей дать количественную оценку при проектировании и эксплуатации сети обслуживания [2,3,4]. Несмотря на то, что опыт проектирования систем безопасности информации еще недостаточно развит, задачи построения СБИ должны решаться на стадии раннего этапа проектирования сети обслуживания. Судя по растущему числу научных работ и компаний, в том числе нефтяных, занимающихся информационной безопасностью в сетях обслуживания, решению этой задачи придается большое значение.

Одной из наиболее очевидных причин нарушения СБИ является умышленный запрос несанкционированного доступа (НСД) к конфиденциальной информации со стороны нелегальных пользователей и последующие нежелательные манипуляции с этой информацией [2–5]. Отметим, что эффективность защиты безопасности информации в сетях обслуживания определяется в основном классом защищенности сети обслуживания [6, 7], который определяет набор механизмов защиты (МЗ), реализованных в сети. Независимо от того, является ли МЗ в составе СБИ аппаратной или программной частью, он может функционировать в постоянном информационном взаимодействии с другими элементами СБИ, оказывая влияние на весь процесс защиты информации.

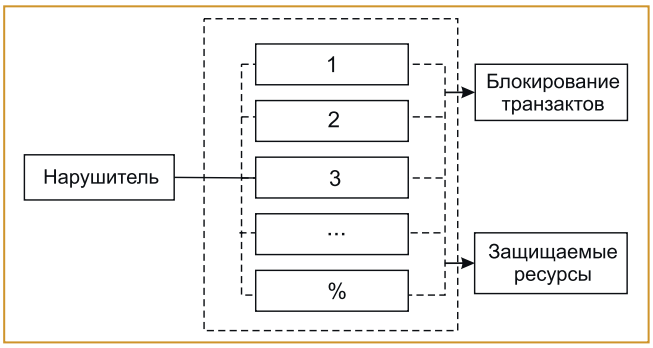

Рис.1. Структура СБИ

Возможность наступления некоторого неблагоприятного события, связанного с надежностными характеристиками МЗ, влекущего за собой различного рода потери, считается риском. Функционирование МЗ описывается следующими возможными состояниями: исправен, неисправен, диагностирован, восстановлен. Подходы, связанные с риском, происходящим от характеристики надежности МЗ, в данном случае не рассматриваются, так как предполагается (как в [1]), что все МЗ считаются надежными.

В данной работе разыскиваются оптимальные конфигурации СБИ без буферной памяти, позволяющие функционировать при ограниченных ресурсах (число параллельно работающих приборов обслуживания (МЗ)). На ранних этапах проектирования подготавливаются результаты с целью построения СБИ (число параллельно работающих приборов обслуживания (МЗ), число запросов НСД в системе, время ожидания запросов НСД в очереди и время пребывания запросов НСД в системе в пределах допустимых потерь запросов), являющиеся оптимальными значениями структурных характеристик СБИ.

В [1] из-за существования факта неполного закрытия системой защиты всех возможных каналов проявления угроз предложена структура СБИ, в которой в отличие от структур [6, 7] всем входным потокам достается МЗ для обслуживания. В данной работе предлагается структура СБИ без буфера, обеспечивающая максимальную информационную безопасность сетей обслуживания путем обеспечения контроля перехода всех запросов НСД от МЗ (рис. 1). Поэтому возникает

задача определения оптимальной конфигурации СБИ, обеспечивающей максимальную степень информационной безопасности сетей обслуживания путем обеспечения контроля перехода всех запросов НСД от МЗ.

В предложенной структуре (рис. 1) нарушитель (злоумышленник, запросы НСД) на входе системы создает разные угрозы с интенсивностью λ. Если один из МЗ свободен, то запрос НСД поступает в этот свободный МЗ, при котором исходный поток НСД разрежается с определенными вероятностями и образует выходной поток. А в случае занятости всех МЗ запрос НСД получает отказ в обслуживании из-за перегрузки системы. Отметим, что СБИ от НСД представляет собой аппаратно-программный комплекс, взаимодействующий с потоками случайных событий, которые обуславливаются действиями злоумышленников, неправильным распределением прав доступа, использованием несанкционированного программного обеспечения, ошибками в программно-технических комплексах идентификации, аутентификации [1,8,9].

При этом преследуется цель разработки математической модели СБИ, позволяющей в силу имеющихся ограниченных ресурсов определить ее оптимальные характеристики. Если рассматривать блок нарушителя как источник информации, а МЗ как параллельно работающие приборы, то СБИ можно рассматривать как однофазную многоканальную систему массового обслуживания (СМО) с потерями.

СБИ состоит из N — числа МЗ, которые осуществляют задержки $\tau_0 = 1/\mu$ на обслуживание, где μ — интенсивность обслуживания запросов НСД.

При обслуживании происходит отсеивание запросов НСД. В СБИ с помощью МЗ выполняется обнаружение с определенной вероятностью и классификация попыток НСД, и реализуются функции блокирования или пропуска запросов НСД к защищаемым ресурсам. Пропущенные (нераспознанные) запросы могут нанести вред защищаемым ресурсам. Защищаемые ресурсы не выполняют самостоятельных функций контроля доступа.

Целью данной работы является поиск оптимальных конфигураций СБИ, позволяющих функционировать при ограниченных ресурсах. Предполагается, что входной поток информации, то есть запросы НСД, являются простейшими, а время обслуживания подчиняется экспоненциальному, постоянному и Эрланговому законам распределения. При этом требуется определить оптимальные значения числа параллельно работающих приборов обслуживания (МЗ), число запросов НСД в СБИ, время пребывания запросов НСД в СБИ в пределах допустимых потерь запросов НСД, происходящих от перегрузки системы.

В качестве критерия эффективности выбрана минимизация математического ожидания вероятности потери запросов НСД в СБИ (то есть вероятность достижения обслуживания всех запросов НСД в МЗ при отсутствии буферной памяти в СБИ).

Постановка задачи и алгоритм анализа характеристик системы с потерями

Общая постановка задачи определения оптимальных характеристик системы с потерями, с ограниченным и неограниченным ожиданиями в [1] сформулирована в следующем виде:

$$M\left[P(\lambda,\mu,N)\right] \to min \quad \text{при } \lambda \ge \lambda_0, \mu \ge \mu_0, N \ge N_0, L_q \le L^0, \tag{1}$$

где M — знак математическое ожидание, $P(\lambda, \mu, N)$ — функция вероятности потери запросов НСД от отказа из-за перегрузки системы обслуживания, L_q — среднее значение длины очереди (величина определяющая объем буферной памяти), λ_0, μ_0, N_0, L_0 — допустимые предельные значения.

В [1] отмечено, что единого строгого аналитического выражения $P(\lambda, \mu, N)$, позволяющего вычислить потери запросов НСД с ограниченными и неограниченными ожиданиями в настоящее время не существует, аналитическое решение задачи (1) представляет большую сложность. Поэтому задача (1) в [1] решена только для системы с ограниченным ожиданием (для СБИ с ограниченным буфером). При этом в качестве функции потери запросов НСД из-за перегрузки системы использована формула Пуассона.

В данной статье представляет интерес минимизация математического ожидания вероятности потери запросов НСД в СБИ (то есть вероятность достижения обслуживания всех запросов НСД в МЗ при отсутствии буферной памяти в СБИ). Тогда задача (1) для системы с потерями (для СБИ без буфера) может выглядеть следующим образом:

$$M\left[P(\lambda,\mu,N)\right] \to min \quad \text{при } \lambda \geqslant \lambda_0, \mu \geqslant \mu_0, N \geqslant N_0, L_q \leqslant 0, \tag{2}$$

где λ_0, μ_0, N_0 — допустимые предельные значения.

Потери запросов НСД происходят из-за отсутствия буферной памяти СБИ. В результате запросы НСД не получают обслуживание и покидают СБИ. В качестве функций вероятности потери запросов НСД в СБИ предлагается использовать функцию потери Эрланга [10]:

$$P(\lambda,\mu,N) = (\rho^N/N!)/\sum_{k=0}^{N}(\rho^k/k!), \tag{3}$$

где $\rho = \lambda/\mu$ — приведенная интенсивность.

Для исследования СБИ как однофазных многолинейных СМО с потерями предлагается вариант алгоритма получения оптимальных значений характеристик системы из [1]. Данный вариант алгоритма отличается от алгоритма в [1] тем, что в качестве функций вероятности потери запросов НСД в СБИ используется функция потери Эрланга, и процесс обслуживания прекращается, когда среднее значение длины очереди удовлетворяет условие $L_q \leqslant 0$. Используя данное условие, по предложенным алгоритмам разыскиваются оп-

тимальные характеристики СБИ без буферной памяти. А после удовлетворения условия $L_q \leqslant 0$ полученные характеристики принимаются как оптимальные характеристики СБИ. Алгоритм включает следующие шаги.

На первом шаге после ввода средних значений λ, μ и установления начального значения $N = N_0$ определяются потери запросов по (3). На последующих шагах определяется число запросов НСД в очереди L_q, и нормализуется соотношение (3) для трех случаев аналитического анализа характеристик системы.

1.Интенсивность поступления и время обслуживания запросов подчиняются экспоненциальному закону. При этом для экспоненциального времени обслуживания [11]:

$$L_q = \frac{\rho^{N+1} / [(N-1)!(N-\rho)]}{(\sum_{k=0}^{N-1} \rho^k / k! + \rho^N [(N-1)!(N-\rho)!])(N-\rho)}.$$

В зависимости от характера объекта $L_q \to \rho^{N+1}/N^2$ при $\rho < 1$, а $L_q \to \rho/(N-\rho)$ при $\lambda/\mu N \to 1$ [9].

При удовлетворении условия $L_q \leqslant 0$ процесс считается нормальным, поэтому полученные характеристики выводятся, и аналитический анализ завершается. В противном случае анализ продолжается, и осуществляется переход ко второму случаю.

2. Интенсивность поступления запросов подчиняется экспоненциальному закону, а обслуживание — постоянному (детерминированному). При неудовлетворении условия $L_q \leqslant 0$ система должна расширить свои возможности путем $N = N + 1$, а при удовлетворении — осуществить переход к третьему случаю. Для постоянного времени обслуживания [11]:

$$L_q = \rho \sum_{m=1}^{\infty} e^{-m\rho} \left[(1 - N/\rho) \sum_{n=mN+1}^{\infty} (m\rho)^n / n! + (m\rho)^{mN} / (mN)! \right]$$

3. Выполнение условия $L_q \leqslant 0$ по постоянному закону обслуживания может оказаться недостаточным для учета некоторых других требований к системе, например, надежности. Поэтому аналитический анализ характеристики системы дополнительно проводится для Эрлангового времени обслуживания [11]:

$$L_q = \rho^2 (1 + 1/k)/(2(1-\rho),$$

где параметр $k = \overline{1,\infty}$.

Для системы Пуассона можно использовать [11]:

$$L_q \approx \left[\begin{matrix} 1 + 0,0830 (\frac{k-1}{k+1})^{0,944} (N-1)^{0,674} ((1-a) + \\ +0,974 N^{0,937} k^{0,0254} (1-a)^{2,04}) \end{matrix} \right] (k+1)\rho^2 / 2k(1-\rho),$$

где $a = \lambda/\mu N$, для больших значений a:

$$L_q \approx \left[\begin{matrix} 1 + \frac{1}{12} (\frac{k-1}{k+1}) (N-1)^{2/3} ((1-a) + \\ +(1-a)^2) \end{matrix} \right] (k+1)\rho^2 / 2k(1-\rho).$$

После определения L_q можно вычислить время ожидания запросов НСД в очереди $\tau_q = L_q/\lambda$, время пребывания запросов НСД в системе $\tau_s = L_s/\lambda$, а < 1, ожидаемое число запросов НСД в системе $L_s = L_q + \rho$.

Таблица 1. Экспоненциальное ВО

N	L	τ_q	τ_s
2	10,2159	11726,9519	25412,6866
3	4,30250	3502,50350	10702,7363
4	2,38030	829,068100	5921,14430
5	2,10580	447,287900	5238,30850
6	1,78410	0,00000000	2479,89880

Таблица 2. Постоянное ВО

N	L	τ_q	τ_s
2	5,5056	5175,7997	13695,5224
3	2,7324	1318,7761	6797,01490
4	2,1393	493,88040	5321,64180
5	1,9955	293,88030	4963,93030
6	1,7841	0,0000000	2479,89880

Таблица 3. Эрланговое ВО

N	L	τ_q	τ_s
2	3,0186	1715,9550	4195,8540
3	2,5058	1003,6161	6233,3333
4	2,1485	506,67590	5337,8109
5	2,0048	306,81500	4987,0647
6	1,7841	0,0000000	2479,8988

Отметим, что выполнение условия $L_q \leqslant 0$ является достаточным для завершения анализа. При невыполнении данного условия осуществляется переход к первому случаю алгоритма при N=N+1.

Численные эксперименты

В работе на основе реальных данных объектов нефтегазодобычи в качестве примера для средних значений λ=1/1410 мс, μ=1/2516 мс и пуассоновского потока запросов НСД по предложенным алгоритмам и составленным программ проведены объемные вычислительные эксперименты. Получены численные результаты для экспоненциального, постоянного и Эрлангового времени обслуживания (табл. 1–3) и (рис. 2–5).

В табл. 1–3 представлена динамика изменения характеристики системы (СБИ) как ожидаемое число запросов НСД в системе $L_S = f(N)$, время ожидания запросов НСД в очереди, время пребывания запросов НСД в системе $\tau_s = f(N)$ для экспоненциального, постоянного и Эрлангового времени обслуживания при N = 2...6. А на рис. 2–4 представлена динамика уменьшения длины очереди запросов НСД $L_q = f(N)$ для экспоненциального, постоянного и Эрлангового времени обслуживания при N = 2...6.

На рис. 5 представлена динамика уменьшения функций вероятности потери запросов НСД в СБИ $P = f(N)$ при N = 2...6.

Анализ полученных результатов (рис. 5) показывает, что значения P удовлетворительно нормализуются при N = 6. Тогда для выбора конкретных значений параметров и характеристик системы могут быть использованы зависимости $L_q = f(N)$ (рис. 2–4). Условие $L_q \leqslant 0$ для всех трех распределений времени обслуживания выполняется лишь при N = 6 (рис. 2–4).

Проверки адекватности аналитических результатов, а также подробный анализ характеристик СБИ при экспоненциальных входных, экспоненциальных, постоянных и Эрланговых выходных потоках для их различных значений и с учетом их трудоемкости осуществлены на основе разработанных на языке GPSS имитационных моделей.

В модели рассматривается однофазная многоканальная система с потерями, в которую на обслуживание поступают пуассоновские входные потоки, а время обслуживания транзактов подчиняется экспоненциальному, постоянному и Эрланговому законам распределения.

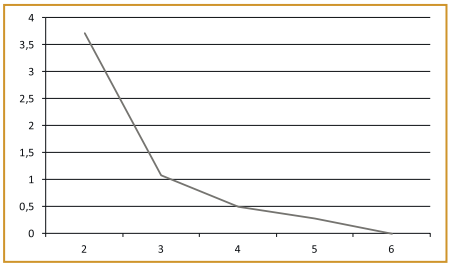

Рис.2

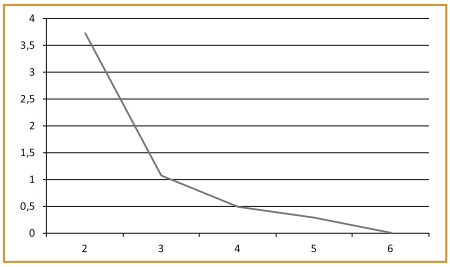

Рис.3

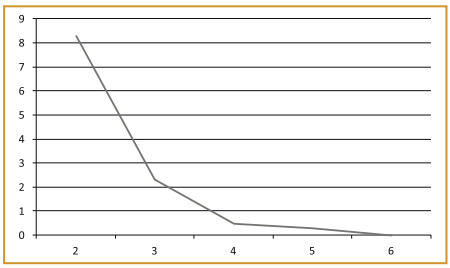

Рис.4

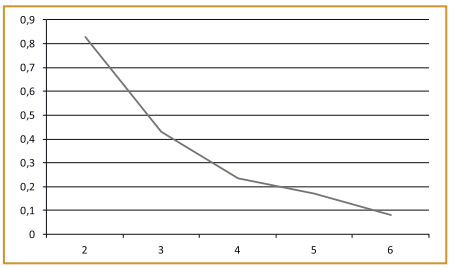

Рис.5

В модели при поступлении транзакта в систему и наличии свободного прибора обслуживания (МЗ) транзакт получает обслуживание. В случае занятости всех МЗ транзакт получает отказ в обслуживании из-за перегрузки системы. Проведены три прогона расчетов по имитационной модели. Полученные результаты показывают, что для трех случаев анализа с учетом всех транзактов при отсутствии очереди на входе СБИ коэффициент использования приборов (МЗ) составляет 0,941; 0,853; 0,765 соответственно. Иными словами приборы обслуживания (МЗ) не простаивают, то есть они загружены в пределах норм, в СБИ происходит удовлетворительное обслуживание.

Сравнительный анализ результатов аналитической модели с результатами имитационной модели показывает, что они хорошо согласованы, и отклонение этих результатов находится в допустимых пределах 2...7%. Полученные результаты могут быть использованы при модификации существующих или построении новых СБИ в сетях обслуживания объектов нефтегазодобычи.

Заключение

В работе предложены вычислительные процедуры и алгоритмы анализа оптимальных значений параметров СБИ как однофазной многоканальной СМО с потерями. Проведены численные эксперименты и получены результаты. С целью проверки адекватности полученных результатов проведены имитационные эксперименты, подтверждающие адекватность численных результатов. Эти результаты могут быть использованы при построении новых или модификации существующих СБИ без буферной памяти в сетях обслуживания объектов нефтегазодобычи.

Данная работа является развитием обобщения рассматриваемых проблем для систем с потерями, с ограниченным и неограниченным объемом буферной памяти (с неограниченным ожиданием).

Список литературы

1. *Исмайлов Б. Г.* Анализ системы безопасности информации в сетях обслуживания объектов нефтегазодобычи//Автоматизация в промышленности. 2020. № 3. с. 16-19.
2. *Зюзин А.С.* Современные тенденции оценки защиты информации // Научный журнал КубГАУ, 2015. №107(03). С.1-12.
3. *Морозова В.И., Врублевский К.Э.* Защита информации в вычислительных системах. Уч. пособие. Под ред. В.И. Морозовой - М.: МИИТ, 2008. 122 с.
4. *Малюк А.А.* Информационная безопасность: концептуальные и методологические основы защиты информации. М.:ГЛТ. 2004. 280 с.
5. *Шаньгин В.Ф.* Информационная безопасность и защита информации. М.:ДМК, 2014.702 с.
6. *Карпова В.В.* Вероятностная модель оценки защищенности средств вычислительной техники с аппаратно-программным комплексом защиты информации от несанкционированного доступа // Программные продукты и системы. 2003. №1. С.31-36.
7. *Карпова В.В.* Методика синтеза оптимального варианта аппаратно-программного комплекса защиты информации от несанкционированного доступа по критерию защищенности // Программные продукты и системы. 2003. № 1. С.36-38.
8. *Григорьев В.А., Карпова А.В.* Имитационная модель системы защиты информации // Программные продукты и системы. 2005. № 2. С.26-30.
9. *Карпова А.В.* Оценка защищенности информации от несанкционированного доступа при помощи имитационной модели системы защиты информации // Программные продукты и системы. 2005. № 2. С.51-54.
10. *Клейнрок Л.* Теория массового обслуживания. Перевод с англ. И.И. Грушко; ред. В.И. Нейман, М.: Машиностроение. 1979. 432 с.
11. *Ахмедов Б. О., Джавадов А. А., Исмайлов С. Ф., Исмайлов Б. Г.* О моделирование и анализе характеристик распределенных мультимикропроцессорных систем//Автоматика и вычислительная техника. 1985. № 3. Рига с. 70-74.

Исмайлов Балами Гасым оглы *– д-р техн. наук, доцент кафедры информационных технологий Национальной Академии Авиации (г. Баку, Азербайджанская Республика).*
E-mail: balemi@rambler.ru

Поступила в редакцию 25.05.2020
Принята в печать 18.06.2020