УДК 621.394.74:519.872

Исмайлов Б.Г., д.т.н.

АНАЛИЗ СИСТЕМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ С НЕОГРАНИЧЕННЫМ ОБЪЕМОМ БУФЕРНОЙ ПАМЯТИ В СЕТЯХ ОБСЛУЖИВАНИЯ

Национальная Академия Авиации, Азербайджан

balemi@rambler.ru

Введение

Работа посвящена подходам к исследованию СБИ в сетях обслуживания, в которой рассматриваются проблемы, характерные для систем с потерями, с ограниченными и неограниченными объемами буферной памяти [1-2]. В отличие от [1-2] здесь анализируются модели, в которых структура системы безопасности базируется на системах безопасности информации (СБИ) с неограниченным объемом буферной памяти.

Значимость проблемы информационной безопасности является признанной, и подтверждением этого являются огромные убытки, понесенные корпорациями из-за недостаточной защищенности информации [3-5].

Современное состояние проблемы в области информационной безопасности и разработки СБИ указывает 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 [3-5]. Следует отметить, что в настоящее время из-за недостаточного развития опыта проектирования систем безопасности информации, задачи построения СБИ должны решаться на стадии раннего этапа проектирования сети обслуживания [1-2]. В настоящее время, учитывая по растущему количеству научных работ и компаний, в том числе, нефтяных, занимающихся информационной безопасностью в сетях обслуживания, данная проблема сохраняет свою актуальность.

Отметим, что 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 [3-6]. Эффективность защиты безопасности информации в сетях обслуживания определяется в основном классом защищенности сети обслуживания [7-8], который определяет набор механизмов защиты (МЗ), реализованных в сети. Следует отметить, что не зависимо 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.

В системе возможность наступления некоторого неблагоприятного события, связанного с надежностными характеристиками МЗ, влекущего за собой различного рода потери, считается риском. Функционирование МЗ описывается следующими возможными состояниями как: исправен, неисправен, диагностирован, восстановлен. Подходы, связанные с риском происходящим от характеристики надежности МЗ, в данном случае не рассматриваются, так как предполагается (как в [1-2]), что все МЗ считаются надежными.

В работе исследуются оптимальные конфигурации СБИ с неограниченным объемом буферной памяти, позволяющие функционировать при ограниченных ресурсах (количество параллельно работающих приборов обслуживания (МЗ)). На ранних этапах проектирования подготавливаются результаты с целью построения

СБИ (количество 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 [1-2] из-за существования факта неполного закрытия системой защиты всех возможных каналов проявления угроз, предложена структура СБИ, т.е. в отличие от структур [7-8] всем входным потокам достается МЗ для обслуживания.

В работе предлагается структура СБИ с неограниченным объемом буферной памяти, обеспечивающая максимальную информационную безопасность сетей обслуживания путем обеспечения контроля перехода всех запросов НСД через МЗ (рис.1).

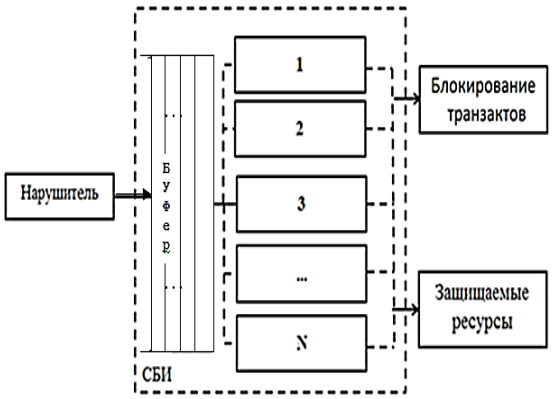

Рис. 1. Структура СБИ

Следовательно, возникает задача определения оптимальной конфигурации СБИ, обеспечивающей максимальную степень информационной безопасности сетей обслуживания путем обеспечения контроля перехода всех запросов НСД через 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 ожидает в очереди в буферной памяти системы до освобождения одного из МЗ. 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 [1-2,9-10]. В работе 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 с неограниченным объемом буферной памяти. 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.

В данной работе осуществляется поиск оптимальных конфигураций СБИ, позволяющих функционировать при ограниченных ресурсах. При этом предполагается, что входной поток информации, то есть запросы НСД, являются простейшими, а время обслуживания подчиняется экспоненциальному, постоянному и Эрланговому законам распределения. В силу данного предположения 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 ожидания в очереди.

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

Постановка задачи и алгоритм анализа характеристик системы с неограниченным объемом буферной памяти

Общая постановка задачи определения оптимальных характеристик системы с потерями, с ограниченным и неограниченным ожиданиями в [1-2] сформулирована в следующем виде:

$$M[P(\lambda,\mu,\mathrm{N})] \rightarrow min \quad (1),$$
$$\text{при } \lambda \geq \lambda_0, \mu \geq \mu_0, N \geq N_0,$$
$$L_q \leq L^0$$

Где M – знак математического ожидания, $P(\lambda,\mu,N)$ – функция вероятности потери запросов НСД от отказа из-за перегрузки системы обслуживания, L_q – среднее значение длины очереди, т.е. величина, определяющая объема буферной памяти, $\lambda_0, \mu_0, N_0, L^0$ – допустимые предельные значения.

В [1-2] отмечено, что единого строгого аналитического выражения$P(\lambda,\mu,N)$, позволяющего вычислить потери запросов НСД с ограниченными, неограниченными ожиданиями и с потерями в настоящее время не существует и аналитическое решение задачи (1) представляет большую сложность. Поэтому задача (1) в [1] решена для системы с ограниченным ожиданием (то есть для СБИ с ограниченным буфером), а в [2] решена для системы с потерями (то есть для СБИ без буфера). При этом в качестве функции потери запросов НСД из-за перегрузки системы в [1] использована формула Пуассона, а в [2] использована функция потери Эрланга.

В отличии от [1-2] данной статье представляет интерес минимизация математического ожидания вероятности потери запросов НСД в СБИ с неограниченным объемом буферной памяти, где $0 < L^0 < \infty$ (то есть вероятность достижения обслуживания всех запросов НСД в МЗ в СБИ с неограниченным объемом буферной памяти).

Потери запросов НСД в такой системе происходят из-за ожидания очереди в буферной памяти СБИ. А в качестве функций вероятности потери запросов НСД в СБИ с неограниченным объемом буферной памяти в отличие от [1-2] предлагается использовать функцию задержки Эрланга [11]:

$$\mathrm{P}(\lambda,\mu,\mathrm{N}) = (\rho^N/[(N-1)!(N-\rho)]/[\sum_{k=0}^{N-1}\rho^k/k! + \rho^N/[(N-1)!(N-\rho)] \quad (2)$$

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

Для исследования СБИ как однофазных многолинейных СМО с неограниченным объемом буферной памяти предлагается вариант алгоритма получения оптимальных значений характеристик системы из [1-2]. Данный вариант алгоритма отличается от алгоритма в [1-2] тем, что в качестве функций вероятности потери запросов НСД в СБИ используется функция задержки Эрланга, и процесс обслуживания прекращается, когда среднее значение длины очереди удовлетворяет условие $L_q \leq L^0$, где $0 < L^0 < \infty$. Используя данное условие, по предложенным алгоритмам разыскиваются оптимальные характеристики СБИ с неограниченным объемом буферной памяти. А после удовлетворения условия $L_q \leq L^0$ 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 (2). На последующих шагах определяется число запросов НСД в очереди L_q, и нормализуется соотношение (2) для трех случаев аналитического анализа характеристик системы.

1. Интенсивность поступления и время обслуживания запросов подчиняются экспоненциальному закону. При

этом для экспоненциального времени обслуживания [12]:

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

В зависимости от характера объекта при$\rho << 1, L_q \to \rho^{N+1}/N^2$и при$\lambda/\mu N \to 1$,

$$L_q \to \rho/(N-\rho).$$

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 случаю.

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 третьему случаю. Для постоянного времени обслуживания [12]:

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

3. Выполнение условий $L_q \le L^0$ 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 [12]:

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

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

Для системы Пуассона можно использовать [12]:

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

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

$$L_q \approx [1 + \frac{1}{12}(\frac{k-1}{k+1})(N-1)^{2/3}((1-a) + (1-a)^2)](k+1)\rho^2/2k(1-\rho)$$

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

Отметим, что выполнение условия при $L_q \le L^0$ 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 $\lambda = 1/1400мс$, $\mu = 1/2498мс$ и $L^0 = 1$ пуассоновского потока запросов НСД по предложенным алгоритмам и составленным программам проведены объемные вычислительные эксперименты. Получены численные результаты для экспоненциального, постоянного и Эрлангового времени обслуживания (табл.1-3) и (рис.2-5).

Таблица 1 Экспоненциальное ВО.

N	L_q	τ_q	τ_s
2	10,310	11827,964	26418,6761
3	4,4026	3603,6030	11712,7364
4	2,4703	834,06820	6120,14438
5	2,2050	448,28890	5338,30850

В табл. 1-3 представлена динамика изменения характеристики системы (СБИ) как ожидаемое число запросов НСД в системе, время ожидания запросов НСД в очереди, время пребывания запросов НСД в СБИ с неограниченным объемом буферной памяти$\tau_s = f(N)$ для экспоненциального, постоянного и Эрлангового времени обслуживания при $N = 2\ldots5$.

Таблица 2. Постоянное ВО.

N	L_q	τ_q	τ_s
2	5,6100	5372,8532	14070,686
3	2,9027	1419,5035	6802,7467
4	2,4803	505,06810	6141,7443
5	2,0020	267,98790	5038,3085

Таблица 3. Эрланговое ВО

N	L_q	τ_q	τ_s
2	3,5100	1926,953	4312,7860
3	2,6027	1302,503	6370,4364
4	2,2803	585,0681	5421,1443
5	2,0054	327,2879	5036,3085

А на рис.2-4 представлена динамика уменьшения длины очереди запросов НСД $L_q = f(N)$ для экспоненциального, постоянного и Эрлангового времени обслуживания при $N = 2\ldots5$.

L_q

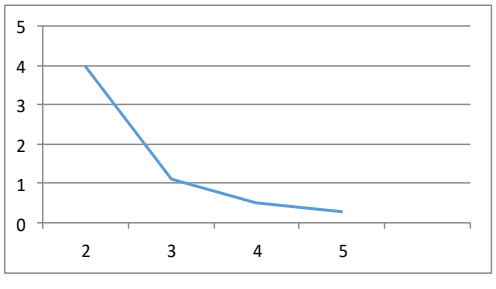

Рис. 2. Зависимость $L_q = f(N)$ для экспоненциального ВО

На рис.5 представлена динамика уменьшения функций вероятности потери запросов НСД в СБИ с неограниченным объемом буферной памяти $P = f(N)$ при$N = 2\ldots5$.

Анализ полученных результатов (рис.5) показывает, что значения P удовлетворительно нормализуются при$N \geq 4$.

L_q

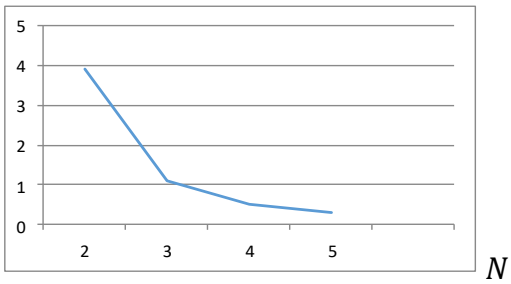

Рис. 3. Зависимост $L_q = f(N)$ для постоянного ВО

L_q

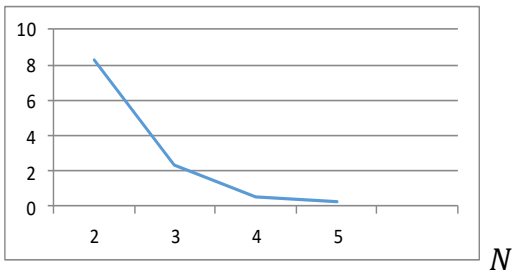

Рис. 4. Зависимость $L_q = f(N)$ для Эрлангового ВО

P

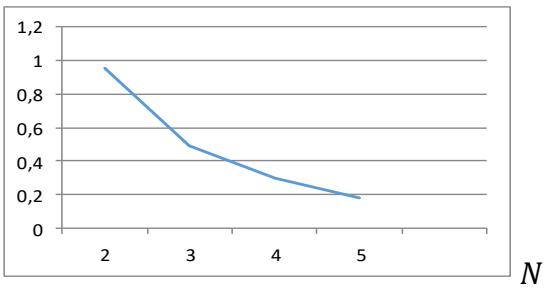

Рис. 5. Зависимость $P = f(N)$

Тогда для выбора конкретных значений параметров и характеристик системы могут быть использованы зависимости $L_q = f(N)$ (см. (рис.2-4). Условие $L_q \leq 1$ для всех трех распределений времени обслуживания выполняется лишь при $N \geq 4$ (рис.2-4).

Проверки адекватности аналитических результатов, а также подробного анализа характеристик СБИ с неограниченным объемом буферной памяти при экспоненциальных входных, экспоненциальных, постоянных и Эрланговых выходных потоков для их различных значений, с учетом их трудоемкости, осуществлены на основе разработанных имитационных моделей на языке GPSS имитационных моделей.

В модели рассматривается однофазная многоканальная система с неограниченным объемом буферной памяти, в которую на обслуживание поступает пуассоновские входные потоки, а время обслуживания транзактов подчиняется экспоненциальному, постоянному и Эрланговому законам распределения.

В модели при поступлении транзакта в систему и наличии свободного прибора обслуживания (МЗ) транзакт получает обслуживание. В случае занятости всех МЗ транзакт ожидает в очереди в буферной памяти системы. Проведены три прогона расчетов по имитационной модели. Полученные результаты показывают, что для трех случаев анализа с учетом всех транзактов и при наличии допустимого количества транзактов в очереди на входе СБИ коэффициент использования приборов (МЗ) составляет 0,952; 0,861; 0,772 соот-

ветственно. Иными словами, приборы обслуживания (МЗ) не простаивают, т.е. они загружены в пределах норм, т.е. 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.

Выводы

Предложены вычислительные процедуры и алгоритмы анализа оптимальных значений параметров СБИ, как однофазной многоканальной СМО с неограниченным объемом буферной памяти. 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 с неограниченным объемом 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).

Литература

1.*Исмайлов Б.Г.* Анализ системы безопасности информации в сетях обслуживания объектов нефтегазодобычи // Автоматизация в промышленности. – №3. – 2020. – С. 16-19.

2.*Исмайлов Б.Г.* Моделирование системы безопасности информации в сетях обслуживания объектов нефтегазодобычи // Автоматизация в промышленности. – №7. – 2020. – С.23-26.

3.*Морозова В.И., Врублевский К.Э.* Защита информации в вычислительных системах. 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. – №1. – 2003. – 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. – № 1. – 2003. – С. 36-38.

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

9.*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.

10.*Клейнрок Л.* Теория массового обслуживания. Перевод с англ. Пер. 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. – Рига, 1985. – №3. – С. 70-74.

Исмайлов Б.Г.

АНАЛИЗ СИСТЕМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ С НЕОГРАНИЧЕННЫМ ОБЪЕМОМ БУФЕРНОЙ ПАМЯТИ В СЕТЯХ ОБСЛУЖИВАНИЯ

Определяется оптимальная конфигурация системы безопасности информации (СБИ), как системы массового обслуживания с неограниченным объемом буферной памяти, обеспечивающая максимальную информационную безопасность сетей обслуживания объектов нефтегазодобычи путем обеспечения перехода всех запросов несанкционированного доступа (НСД) от механизма защиты (МЗ). Разработаны вычислительные процедуры и алгоритмы исследования оптимальных характеристик СБИ как однофазных многоканальных систем массового обслуживания (СМО) с неограниченным объемом буферной памяти. Проведены вычислительные эксперименты и получены численные результаты, которые позволяют использовать их при построении СБИ в сетях различного назначения.

Ключевые слова: *системы безопасности информации, системы с неограниченным объемом буферной памяти, механизм защиты, несанкционированный доступ, системы массового обслуживания, время обслуживания.*

Ismailov B.G.

ANALYSIS OF INFORMATION SECURITY SYSTEM WITH UNLIMITED BUFFER MEMORY IN SERVICE NETWORKS

The optimal confiquration of the information security system (ISS) is determined as a queuing system with an unlimited amount of buffer memory, which ensures the maximum information security of service networks for oil and gas production facilities by ensuring the transition of all unauthorized access requests (UA) from the security protection mechanism (PM).

Computational procedures and algorithms have been developed for studying the optimal characteristics of ISS as single-phase multi-channel queuing systems (QS) with an unlimited amount of buffer memory. Computational experiments have been carried out and numerical results have been obtained, which make it possible to use them in the construction of ISS in networks for various purpose.

Keywords: *information security systems, systems with unlimited buffer memory, protection mechanism, unauthorized access, queuing systems, service time.*