DOI: 10.25728/avtprom.2020.03.04

Анализ 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). Проведены вычислительные эксперименты и получены численные результаты, которые позволяют использовать предложенный подход при построении СБИ в сетях различного назначения.

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

Введение

Одним из наиболее распространенных видов угроз в сетях обслуживания является несанкционированный доступ (НСД), заключающийся в получении доступа к ресурсу, на который у него нет разрешения в соответствии с принятой в нефтяной компании политикой безопасности. Эффективность безопасности информации в сетях обслуживания определяется в основном классом защищенности сети обслуживания [1,2], который определяет набор механизмов защиты (МЗ), реализованных в сети.

В работах [3–6], которые предлагают методы и методики, позволяющие выполнять количественную оценку защищенности информации при использовании системы безопасности информации (СБИ) на базе определенного набора вероятностных показателей.

Для обоснования методики оценки защищенности информации в [3,4] разработана теоретическая модель СБИ от НСД, при котором исходный поток запросов на НСД разрежается с определенными вероятностями и образует выходной поток.

Однако в работах [3,4] отмечается, что существует факт неполного закрытия системой защиты всех возможных каналов проявления угроз, то есть не для всех заявок из входного потока срабатывает механизм защиты (МЗ). В результате запросы НСД не проходят проверки средств защиты и пропускаются к защищаемому ресурсу, что в итоге реализует соответствующую угрозу. Поэтому возникает задача определения оптимальной конфигурации СБИ, обеспечивающей максимальную информационную безопасность сетей обслуживания путем обнаружения механизмами защиты всех запросов НСД.

Для решения поставленной задачи предлагается новая структура СБИ (рис. 1), отличная от аналогов [3–6].

В структуре нарушитель (злоумышленник) генерирует запросы НСД на входе системы с интенсивностью. СБИ представляет собой аппаратно-программный комплекс, взаимодействующий с потоками случайных событий, которые обуславливаются рядом причин типа:

— действиями злоумышленников;

— неправильным распределением прав доступа;

— использованием несанкционированного программного обеспечения;

— ошибками в программно-технических комплексах идентификации, аутентификации и т. д.

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.

СБИ состоит из общего буфера для ожидания в очереди запросов НСД за некоторое время τ_q, которые осуществляют задержки $\tau_0 = 1/\mu$ на обслуживание,

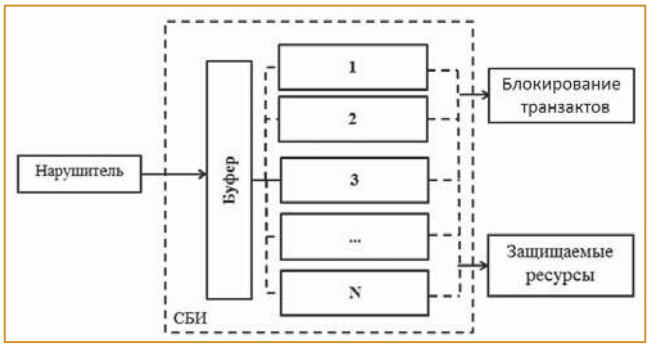

Рис. 1. Структура системы безопасности информации

где μ- интенсивность обслуживания запросов НСД и N- число МЗ.

При обслуживании происходит отсеивание запросов НСД. В СБИ со стороны МЗ выполняется обнаружение и классификация попыток НСД с определенными вероятностям и исполняются функции блокирования или пропуска запросов НСД к защищаемым ресурсам. Пропущенные (нераспознанные) запросы могут нанести вред защищаемым ресурсам. Защищаемые ресурсы не выполняют самостоятельных функций защиты.

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 закону распределения.

Таблица 1. Экспоненциальное время ожидания

N	L_s	τ_q	τ_s
2	10,2159	11726,9519	25412,6866
3	4,3025	3502,5035	10702,7363
4	2,3803	829,0681	5921,1443
5	2,1058	447,2879	5238,3085

Таблица 2. Постоянное время ожидания

N	L_s	τ_q	τ_s
2	5,5056	5175,7997	13695,52.24
3	2,7324	1318,7761	6797,0149
4	2,1393	493,8804	5321,6418
5	1,9955	293,8803	4963,9303

Таблица 3. Время ожидания по теории Эрланга

N	L_s	τ_q	τ_s
2	3,0186	1715,9550	4195,8540
3	2,5058	1003,6161	6233,3333
4	2,1485	506,6759	5337,8109
5	2,0048	306,815	4987,0647

При этом требуется определить оптимальные характеристики таких систем: длину очереди определяющей объем памяти (буфера), число параллельно работающих приборов обслуживания (МЗ), число запросов в системе, время ожидания запросов в очереди и время пребывания запросов в системе в пределах допустимых потерь запросов.

Замечание. МЗ в составе СБИ, являясь аппаратной частью, могут функционировать в постоянном информационном взаимодействии с программной частью, оказывая влияние на весь процесс защиты информа-ции. Возможность наступления некоторого неблагоприятного события, связанного в основном с надежностными характеристиками МЗ, влекущего за собой различного рода потери, считается риском. Функционирование МЗ описывается следующими возможными состояниями: исправен, неисправен, диагностирван, восстановлен. Подходы, связанные с риском в данном случае не рассматриваются, так как предполагается, что все МЗ являются надежными.

Разработка математической модели СБИ

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

$$M\left[P(\lambda,\mu,N)\right]\to min \qquad (1)$$

$$\text{при } \lambda\ge\lambda_0,\mu\ge\mu_0,N\ge N_0,$$
$$L_q\le L_0$$

где λ_0, μ_0, N_0, L_0 — допустимые предельные значения.

Данная задача может быть решена для системы с потерями запросов, с ограниченными и неограниченными ожиданиями. Однако единого строгого аналитического выражения $P(\lambda, \mu, N)$, позволяющего вычислить потери запросов НСД для этих систем в настоящее время не существует и, соответственно, аналитическое решение постановки (1) представляет большую сложность.

Поэтому учитывая сложный характер по обслуживанию запросов НСД (отсеивание запросов НСД, обнаружение и классификация попыток НСД, блокирования или пропуска запросов НСД к защищаемым ресурсам и т.д.) предлагается решение постановки задачи (1) для системы с ограниченным ожиданием, то есть данная система имеет ограниченное место в буфере СБИ. Потери вида (1) для системы с ограниченным ожиданием определяются формулой Пуассона [7]:

$$P(\lambda,\mu,N)=\sum_{i=N}^{\infty}(\rho^i/i!)e^{-\rho}, \qquad (2)$$

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

Значения числа заявок L_q для экспоненциального времени обслуживания могут быть определены следующим образом [6]:

$$L_q=P_1(\rho/(N-\rho)), \qquad (3)$$

где P_1-функция задержки Эрланга, которая определяется следующей форулой [7]:

$$P_1=\frac{\rho^N/\left[(N-1)!(N-\rho)\right]}{\sum_{k=0}^{N-1}\rho^k/k!+\rho^N\left[(N-1)!(N-\rho)!\right]}.$$

В зависимости от характера объекта применения системы может допускать следующие аппроксимации [8]:

$$\text{при } \rho\ll 1 \quad L_q\to\rho^{N+1}/N^2, \qquad (4)$$

$$\text{при } \lambda/\mu N\to 1 \quad L_q\to\rho/(N-\rho). \qquad (5)$$

Для постоянного времени обслуживания

$$L_q=\rho\sum_{m=1}^{\infty}e^{-m\rho}\left[(1-N/\rho)\sum_{n=mN+1}^{\infty}(m\rho)^n/n!+(m\rho)^{mN}/(mN)!\right]. \qquad (6)$$

Для Эрлангового времени обслуживания

$$L_q=\rho^2(1+1/k)/(2(1-\rho)), \qquad (7)$$

где параметр $k=\overline{1,\infty}$.

Для системы Пуассона можно использовать [8]:

$$L_q\approx\left[\begin{array}{l}1+0,0830(\frac{k-1}{k+1})^{0,944}(N-1)^{0,674}((1-a)+\\+0,974N^{0,937}k^{0,0254}(1-a)^{2,04})\end{array}\right](k+1)\rho^2/2k(1-\rho), \qquad (8)$$

где $a=\lambda/\mu N$.

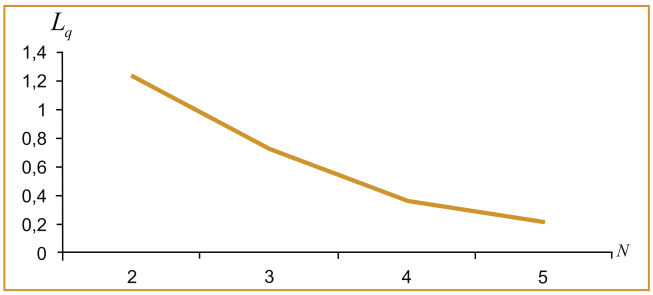

Рис. 2. Зависимость $L_q = f(N)$ для экспоненциального времени ожидания L_q

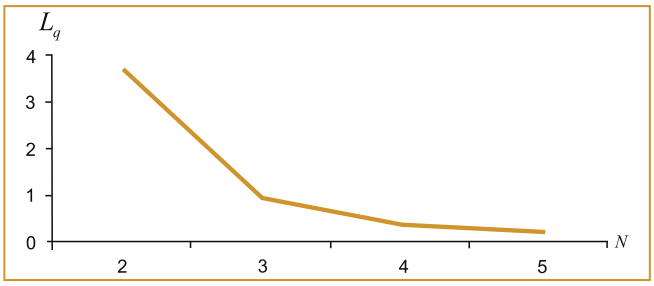

Рис. 3. Зависимость $L_q = f(N)$ для постоянного времени ожидания L_q

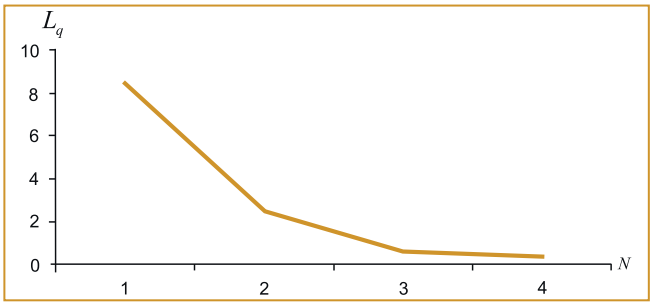

Рис.4. Зависимость $L_q = f(N)$ для Эрлангового времени ожидания P

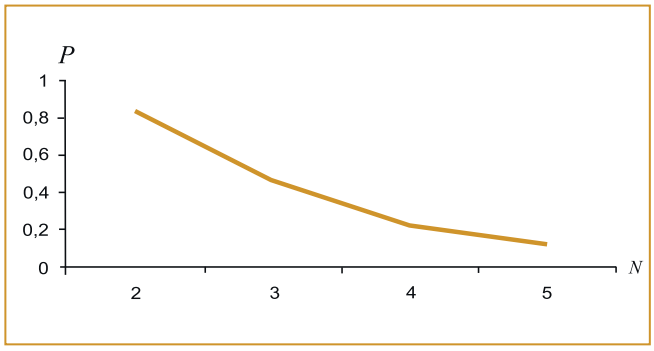

Рис. 5. Зависимость $P = f(N)$

Для больших значений а получим выражение:

$$L_q \approx \left[1+\frac{1}{12}\left(\frac{k-1}{k+1}\right)(N-1)^{2/3}((1-a)+(1-a)^2)\right](k+1)\rho^2/2k(1-\rho). \quad (9)$$

При известном L_q можно определить также время ожидания запросов в очереди: $\tau_q = L_q/\lambda$, время пребывания запросов в системе: $\tau_s = L_s/\lambda$, $\lambda/\mu N < 1$; ожидаемое число запросов в системе: $L_s = L_q + \rho$.

Алгоритм анализа характеристик СБИ

На основе приведенного математического аппарата для исследования СБИ как однофазных многолинейных СМО разработан алгоритм получения оптимальных значений характеристик системы, который 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 по (2). На последующих шагах это соотношение нормализуется для трех случаев аналитического анализа характеристик.

1. Интенсивность поступления и время обслуживания 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 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 путем $N=N+1$, а при удовлетворении — осуществить переход к третьему случаю.

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 характеристик системы проводится дополнительно для экспоненциальных входных запросов и времени обслуживания по теории Эрланга. Выполнение условия $L_q \le L_0$ является достаточным для завершения анализа. При невыполнении данного условия осуществляется переход к первому случаю алгоритма при $N=N+1$.

Численные эксперименты

В качестве примера на основе реальных данных объектов нефтегазодобычи для средних значений λ=1/1390 *мс*, μ=1/2480 *мс*, и L_0=1 пуассоновского потока заявок по приведенным формулам (2) — (9) создана компьютерная программа. Полученные результаты для экспоненциального, постоянного и Эрлангового значений времени обслуживания приведены в виде табл. 1–3 и на рис. 2–4.

Из рис. 5 видно, что значения удовлетворительно нормализуются при значениях $N = 4,5$.Тогда для выбора конкретных значений параметров и характеристик системы $(L_q, L_s, \tau_q, \tau_s)$, могут быть использованы зависимости $L_q = f(N)$ (таб.1–3), при которых значения нормализуются. Как видно, что условие $L_q \le L_0$ для всех трех распределений времени обслуживания выполняется лишь при $N \geqslant 4$. Значение N=5 может

дать удовлетворительное обслуживание даже при возможных простых неисправностях.

С целью проверки адекватности аналитических 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 транзакций подчиняются экспоненциальному, постоянному и Эрланговому законам распределения соответственно. В модели транзакции образуют ограниченную очередь в буферной памяти.

Полученные результаты показывают, что для трех случаев анализа средняя длина очереди составляет 2,00031; 2,03013; 2,00142 соответственно, среднее время ожидания в очереди с учетом всех транзакций по аналогии составляет 4126, 021; 1819,75; 882,50, а коэффициент использования каналов составляет 0,891; 0,774; 0,703 соответственно. Отклонение Δ результатов аналитического (A) и имитационного (I) моделирования определяется как $\Delta = \left[\left|I - A\right| / A\right] 100\%$.

Сравнительный анализ результатов аналитической модели с результатами имитационной модели показывает, что они хорошо согласованы, а полученные результаты могут быть использованы при построении СБИ в сетях объектов нефтегазодобычи.

Заключение

В работе предложены вычислительные процедуры и алгоритмы анализа оптимальных значений параметров СБИ как однофазной многоканальной системы массового обслуживания с ограниченной буферной памятью при экспоненциальных входных, экспоненциальных, постоянных и Эрланговых выходных потоков. Проведены численные и имитационные эксперименты. Результаты имитационного моделирования подтверждают адекватность численных результатов. Эти результаты могут быть использованы при построении новых или модификации существующих СБИ в сетях обслуживания объектов нефтегазодобычи. В настоящее время проводятся исследования по обобщению разработанных процедур решения рассматриваемых проблем для систем с потерями, с ограниченным и неограниченным объемом буферной памяти.

Список литературы

1. *Малюк А.А.* Информационная безопасность: концептуальные и методологические основы защиты информации. М.:ГЛТ. 2004.280 с.
2. *Шаньгин В.Ф.* Информационная безопасность и защита информации. М.:ДМК, 2014.702с.
3. *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.
4. *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.
5. *Григорьев В.А., Карпова А.В.* Имитационная модель системы защиты информации // Программные продукты и системы. 2005. № 2. С.26-30.
6. *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.
7. *Клейнрок Л.* Теория массового обслуживания. Перевод с англ. И.И. Грушко; ред. В.И. Нейман, М.: Машиностроение. 1979. 432с.
8. *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. с. 70-74.

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

Точность в миллисекунды: инструмент Sandvik Coromant для часов Bremont

Британский производитель часов класса люкс, компания Bremont, смогла увеличить объем выпускаемой продукции в два раза благодаря внедрению комплексного производственного модуля из пятиосевого обрабатывающего центра от DMG MORI и оснастки от компании Sandvik Coromant.

Производство часовых механизмов связано с работой с небольшими деталями - безелями, корпусными колесами и корпусами из нержавеющей стали. Найти инструмент для обработки столь малых по размеру резьб и различных отверстий сложно. Стоимость продукции и ее объем при этом высоки, что не оставляет Bremont шанса на ошибку.

Во время подготовки производства шести новых моделей часов компания Sandvik Coromant предоставила инженерам DMG MORI достаточное число единиц оснастки, чтобы те смогли разработать и изготовить специальные оправки для противошпинделя и запрограммировать станки в CAM-системе. В результате, на заводе Bremont был установлен станок NTX 1000 от DMG MORI, оснащенный поворотным устройством, содержащим 30 единиц инструментальной оснастки с интерфейсом Sandvik Coromant Capto®. Оснастка предлагает возможность расширения емкости до 76 единиц, а два шпинделя позволяют выполнять токарную и пятиосевую высокоскоростную фрезерную обработку одновременно.

Полный производственный цикл для компонентов часов был запущен сразу после установки. Все этапы изготовления готового компонента от черновой обработки заготовки из нержавеющей стали до финишной отделки проходят круглосуточно без участия оператора.

Модульная быстросменная инструментальная оснастка Coromant Capto позволяет использовать одни и те же инструменты во всех цехах за счет непосредственного интегрирования системы в шпиндель и большого разнообразия удлинителей и переходников. Соединение оснастки предлагает шесть типоразмеров для любой области применения: C3-C10, с диаметром фланца 32, 40, 50, 63, 80 и 100 мм. Coromant Capto снижает потребность в дорогостоящих специальных инструментах с длительными сроками поставки, а также время наладки и смены инструмента, что обеспечивает значительный рост коэффициента использования станка.

Http://mant.com