УДК 621.3.089

В.М.Буртняк, к.т.н.

МОДЕЛЬ ОЦЕНКИ ВРЕМЕННЫХ ПАРАМЕТРОВ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В СИСТЕМАХ КОНТРОЛЯ И СЛЕЖЕНИЯ ЗА ХРАНЕНИЕМ ЯДЕРНЫХ МАТЕРИАЛОВ

The model of estimation of temporal parameters of informative processes is offered in the checking and track after storage of nuclear materials systems. Application of model allows operatively to calculate temporal descriptions of the system at its planning.

Системы автоматического контроля и слежения (САКС) за хранением ядерных материалов предназначены для прогноза, предотвращения и обнаружения угроз совершения террористических актов [1] с целью обеспечение безопасности особо опасных техногенных объектов, к которым и относятся ядерные материалы.

Качество функционирования и использования средств САКС в условиях крупных производств, техногенных объектов, со сложной топологией расположения большого количества контролируемых объектов определяется эффективностью организации систем контроля и слежения и управления режимами контроля на основе мониторинга общего состояния объектов [2].

Для более эффективного взаимодействия все САКС при большом количестве контролируемых объектов объединяются в единую интегрированную систему безопасности (ИСБ). Такая интеграция обуславливает острую необходимость создания методов и средств построения систем на основе общих критериев и принципов с учетом современного уровня развития науки и техники.

Особую актуальность на современном этапе приобретает проблема разработки методологических принципов построения САКС для класса сложных техногенных объектов, характеризуемых сложным математическим описанием и дефицитом информации, необходимой и доступной для контроля.

Практически все ИСБ имеют одну общую цель - это удовлетворение потребностей пользователей в обеспечении надежного и своевременного представления полной, достоверной и конфиденциальной информации о состоянии контролируемого объекта. Степень выполнения этих потребностей характеризует качество функционирования ИСБ.

Обеспечение качества современных ИСБ и САКС немыслимо без применения моделей, позволяющих оценивать и оптимизировать процессы сбора, хранения и обработки информации. Чтобы понять, как проектировать ИСБ, научится ею управлять, определять наилучшие стратегии защиты техногенного объекта и прогнозировать последствия угроз террористических

 © В.М.Буртняк

актов приводит к необходимости математического моделирования.

Функционирование ИСБ можно представить в виде следующих элементарных операций информационного процесса:

- сбор, преобразование информации о состоянии контролируемого объекта;
- анализ исходной информации (предварительная обработка и поиск потенциальных угроз);
- передачу информации на центральный пост наблюдения;
- принятие решений о состоянии контролируемого объекта;
- поиск методов защиты от потенциальных угроз;
- хранение измерительной информации, методов защиты и правил выбора методов защиты;
- предоставление информации пользователю.

Все многообразие операций выполняемых в ИСБ характеризуется прежде всего временными характеристиками. В этом контексте оценка временных параметров потока и заявок по наблюдениям над периодом занятости системы является важной задачей при проектировании системы. Основными показателями временных свойств информационных процессов ИСБ относятся:

- среднее время выполнения информационного процесса (среднее время реакции системы на возникшее событие);
- продолжительность временного интервала, в течение которого информационный процесс завершается с заданной вероятностью.

Для оценки своевременности представления по событиям выходной информации в ИСБ можно использовать модели системы массового обслуживания (СМО) (рис. 1). В терминах СМО ИСБ можно описать следующим образом.

Заявки на обслуживание поступают через случайные интервалы времени в виде событий от следующих источников:

- САКС - информация о состоянии контролируемого объекта;
- Пользователей – получение выходной информации.

Вычислительная система «центральный пост» обслуживает эти заявки. Обслуживание длится некоторое время. В результате конкуренции различных событий за информационные и программные ресурсы могут возникнуть очереди на обслуживание, при этом заявка помещается в буфер и ждет там начала обслуживания. Предполагается что буфер имеет такую длину, что в системе отсутствуют переполнения и гарантируется отсутствие информационных потерь. События из очереди обслуживаются согласно принятой технологии обработки. Когда подходит очередь обработки события, подключается требуемая к выполнению функциональная задача. Моментом окончания обработки события является представление пользователю некоторого выходного документа. Под временем обработки события понимается не только время, необходимое для получения одного

выходного документа, но и время, необходимое для получения по событию совокупности нескольких выходных документов.

Дисциплина обслуживания буфера в нашем случае смешанная: обслуживание по приоритетам и в очереди с одинаковыми приоритетами по алгоритму FIFO (First Input - First Output) первым пришел - первым обслужен.

Процессы обработки событий в ИСБ формируются как процессы массового обслуживания в приоритетной системе с бесконечным числом мест для ожидания и произвольной функцией распределения времени обработки запросов [3].

Поток событий может быть определен тремя эквивалентными способами:

- Последовательностью моментов времени t_1 ,t_2 ,…,t_n наступления событий;
- Последовательность промежутков времени между событиями Δt_1 ,Δt_2 ,…, Δt_n;

Последовательностью чисел k_1 ,k_2 ,…,k_n, определяющих количество событий, наступивших в течение заданного отрезка времени [t_0 ,t_1), [t_0 ,t2),…, [t0 ,tn).

Потоки событий в ИСБ характеризуются следующими свойствами: стационарностью, без последствий и ординарностью. Такой поток называется простейшим (пуассоновским) потоком.

Однако при критическом изучении условий функционирования событий в ИСБ, может показаться, что у нас имеется совершенно не пуассоновский поток. Например, зачастую нарушается ординарность – одновременно происходят несколько событий (событие от САКС и запрос пользователя). Условие стационарности так же часто не выполняется, например, меняется интенсивность заявок на обработку событий. Не соблюдается условие «без последствия», например, выход из строя сервера «центрального поста» (из-за увеличения нагрузки), который может привести к отказу всей системы безопасности.

В действительности это не так. Предположение о пуассоновском распределении потоков заявок на обработку в систему может быть обосновано тем, что среди всех простейших потоков пуассоновский поток ставит систему обслуживания в наиболее жесткие условия функционирования и для показателей времени ожидания запросов в очередях дает верхние оценки. Более того, потоки запросов одного типа представляют собой, как правило, сумму большого числа потоков от различных источников. Интенсивность каждого из слагаемых потоков мала по сравнению с интенсивностью суммарного потока. В этой ситуации действует предельная теорема Хинчина А.Я. [5] о сходимости сумм ступенчатых процессов к пуассоновскому. Хинчин А.Я. доказал, что если поток является суммой большого числа n независимых ординарных, стационарных потоков интенсивности которых λ_i $(i = \overline{1,n})$ и ни один из них не является

сравнимым по мощности со всем суммарным потоком, то при некоторых аналитических ограничениях суммарный поток сходится к простейшему с интенсивностью $\lambda = \sum_{i=1}^{n} \lambda_i$

Все приведенные соображения, а также результаты статистических исследований, проводимые в ходе испытаний системы, свидетельствуют о возможности использования допущения о пуассоновости потоков заявок на обслуживание.

Т.е. мы имеем систему массового обслуживания типа $M/G/\infty$ - систему с бесконечным числом приборов, на которую поступает пуассоновский поток заявок интенсивности λ.

Предположение о бесконечности числа мест для ожидания обработки события означает на практике выделение для хранения событий, входной и выходной информации таких объемов памяти буферов и базы данных, которые при правильной эксплуатации гарантируют отсутствие информационных потерь в системе вследствие их возможного переполнения

Вероятность Pi(Δt) поступления i заявок в систему за время Δt при нормальном распределении входных заявок определяется формулой

$$P_i(\Delta t) = \frac{(\lambda \Delta t)^i}{i!} \cdot e^{-\lambda \Delta t}, \quad (1)$$

Здесь λ - интенсивность поступления потока событий (заявок), которая определяется как среднее число поступлений событий в систему.

При независимости промежутков Δt k (k=1,2,…) между событиями:

$$P(\Delta t_k < x) = 1 - e^{-\lambda \Delta t}, \quad (2)$$

Плотность распределения вероятностей промежутков времени между событиями подчинена показательному закону:

$$p_x(x) = \begin{cases} \lambda e^{-\lambda x}, \text{x} \geq 0 \\ 0, \text{x} < 0 \end{cases}, \quad (3)$$

Математическое ожидание промежутка Δt между событиями:

$$M_{\Delta t} = \frac{1}{\lambda}, \quad (4)$$

Дисперсия промежутка Δt между событиями:

$$D_{\Delta t} = \frac{1}{\lambda^2}, \quad (5)$$

Среднеквадратическое отклонение промежутка Δt:

$$\sigma_{\Delta t} = \sqrt{D_{\Delta t}} = \frac{1}{\lambda^2}, \quad (6)$$

Математическое ожидание числа событий за промежуток Δt:

$$M_i = \lambda \Delta t \,, \qquad (7)$$

Дисперсия числа событий за промежуток Δt:

$$D_i = \lambda \Delta t \,, \qquad (8)$$

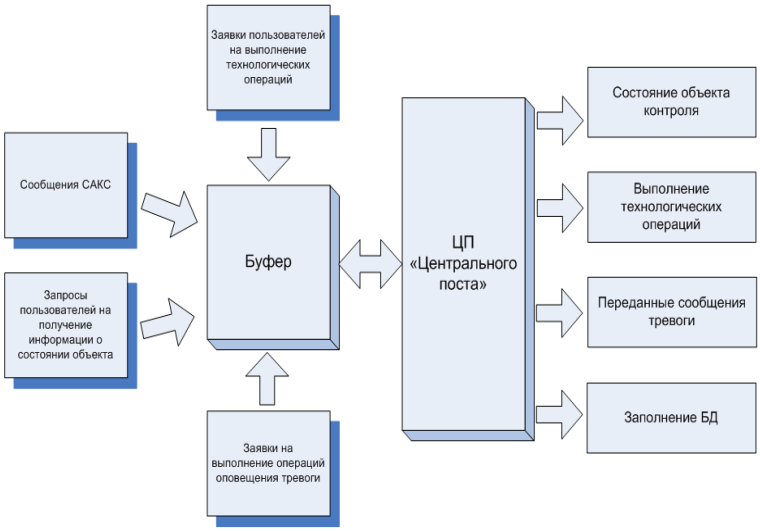

Рис. 1. Модель процессов массового обслуживания ИСБ

Одноканальная экспоненциальная СМО ИСБ задается параметрами λ и $T_{ож}$ [4].

$T_{ож}$- среднее временя обслуживания заявки. В нашем случае равняется $1/\lambda$.

Анализ такой СМО заключается в расчете следующих характеристик:

- коэффициент загрузки ρ;
- средняя длина *L* очереди;
- среднее число *M* заявок в ИСБ;
- среднее время $\overline{T}ож$ ожидания обслуживания;
- среднее время $\overline{T}пр$ пребывания заявки в СМО ИСБ.

Коэффициент загрузки рассчитывается по формуле

$$\rho = \lambda \, \overline{T}ож \qquad (9)$$

Если выполняется условие

$$\rho \le 1, \qquad (10)$$

то СМО функционирует в штатном режиме при котором, все вероятностные характеристики системы являются постоянными во времени величинами. Сами происходящие в СМО события остаются при этом случайными. Если (10) не выполняется, то штатного режима у СМО не существует.

В штатном режиме среднее число *M* заявок в СМО постоянно. Поэтому среднее число заявок, приходящих в СМО в единицу времени, равно среднему числу заявок, в единицу времени, уходящих из СМО. Следовательно, в штатном режиме интенсивность потока уходящих заявок равна λ. Коэффициент загрузки ρ в стационарном режиме есть:

- среднее значение той части единицы времени, в течение которой канал занят;
- вероятность того, что канал занят;
- среднее число заявок в канале.

В последующем речь будет идти только о значениях характеристик штатного режима.

Средняя длина очереди (среднее число заявок в очереди) в одноканальной экспоненциальной СМО рассчитывается по формуле:

$$L = \frac{\rho^2}{1-\rho} \tag{11}$$

Среднее число M заявок в СМО равно сумме среднего числа L заявок в очереди и среднего числа ρ заявок в канале:

$$M = \frac{\rho}{1-\rho} \tag{12}$$

Заявка перемещается в очереди в среднем с постоянной скоростью. Среднее число переходов заявки в очереди на одно место вперед за единицу времени равно ρ.

При такой скорости перемещения L переходов произойдет за время, равное в среднем:

$$\overline{T}ож = \frac{\overline{T}обс \cdot \rho}{1-\rho} \tag{13}$$

Формула (13) дает среднее время прохождения заявки через очередь. Это и есть среднее время ожидания.

Среднее время пребывания заявки в СМО ИСБ есть сумма среднего времени ожидания и среднего времени обслуживания заявки:

$$\overline{T}пр = \frac{\overline{T}обс}{1-\rho} \tag{14}$$

Вероятность наличия в системе k требований определяется с помощью геометрического закона распределения в виде

$$(1 - \rho)\rho^k, \quad k = 0,1,2,...$$

Характеристики (9-14) дают ценную информацию о моделируемой в виде СМО системе. В нашем случае ρ равен коэффициенту использования (занятости) центрального процессора системы, а (1- ρ) коэффициенту простоя. При проектировании системы необходимо закладывать ресурс такой, чтобы коэффициент использования был достаточно велик. Величина

$\overline{T}пр$ характеризует среднее время, в течение которого программы по обслуживанию событий в системе ожидают освобождения центрального процессора. В это время программы фактически "простаивают". Желательно, чтобы $\overline{T}пр$ было достаточно мало.

Представленная модель ориентирована на обеспечение выполнения требований стандартов и анализ случайных процессов, физически свойственных интегральным системам безопасности независимо от их функционального приложения. Применение модели позволяет оперативно вычислять временные характеристики системы, а также аргументировано обосновывать количественные требования технического задания к характеристикам системы при ее проектировании. Модель позволяет оценить выполнение требований заказчика и выявлять «узкие места» и уязвимости системы.

1. *Белоус В. Ядерный терроризм в современном мире.- Ядерная безопасность. – 2000. - № 34-35.*
2. *Забулонов Ю.Л., Лисиченко Г.В. Нові засоби оперативного контролю за нерозповсюдженням ядерно - радіаційних матеріалів // Сб. науч. тр. СНИЯЭиП. – Севастополь, 2005. - Вып. 12. – С. 31-38.*
3. *Гихман И.И., Скороходов А.В. «Теория случайных процессов» М 1973 г.*
4. *Корн Г., Корн Т. «Справочник по математике для научных работников и инженеров» Издательство «Наука» М 1973 г.*
5. *Хинчин А.Я. Работы по математической теории массового обслуживания. М. 1963 г*

Поступила 29.01.2009р.

УДК 004.087.5

А.М. Давиденко, В.В. Душеба, Р.В. Яровий

АНАЛІЗ ВРАЗЛИВОСТЕЙ СМАРТ-КАРТ В АСПЕКТІ МОДЕЛЮВАННЯ СИСТЕМ ЗАХИСТУ НА ЇХ ОСНОВІ

The analysis of vulnerability of intellectual cards is conducted, as a constituent of the informatione system

Вступ. Смарт-ка́ртка (англ. *smart card*) — пластикова картка, що містить інтегральну схему, яка забезпечує певний рівень програмованості та невеликий обсяг пам'яті.

Смарт-карти використовуються для ідентифікації, одно- і двофакторної автентифікації користувачів, зберігання ключової інформації та проведення

 © А.М. Давиденко, В.В. Душеба, Р.В. Яровий