Эвристическая модель ликвидации нештатных ситуаций в эргатических системах управления

Heuristic model of elimination of emergencies in ergatic management systems

Смагин / Smagin V.
Владимир Александрович
(va_smagin@mail.ru)
доктор технических наук, профессор,
заслуженный деятель науки РФ,
действительный член МАИ.
ФГКВОУ ВО «Военно-космическая академия
имени А. Ф. Можайского» МО РФ,
профессор кафедры метрологического обеспечения.
г. Санкт-Петербург

Ключевые слова: автоматизированная система управления – automated control system; информационная подсистема – information subsystem; сложный организационно-технический объект – complicated organizational and technical object; показатели качества функционирования – functioning figures of merit; информационные услуги – information services; экспертный опрос – expert inquiry; функция полезности – utility function.

Предложена модель для ликвидации нештатной ситуации при работе системы. Модель основана на предварительном обучении и тренировке операторов управления ликвидации нештатной ситуации до начала работы системы.

For support of the required indices of efficiency and continuity of difficult organizational and technical objects control within the automated control system (ACS) they create a developed information subsystem which provides receiving necessary information services to officials of governing bodies and complexes of the ACS automation equipment. In this article, the main attention is paid to issues of a choice and reasons for figures of merit of functioning of information subsystem of ACS by difficult organizational and technical objects.

Введение

Современные сложные системы управляются, организуются, контролируются, обслуживаются и т.д. человеком или группой людей – операторов. Правильно осуществляемое между ТС и ЧС взаимодействие определяет максимально достижимый эффект. Этот эффект может быть экономическим, политическим. Во многих случаях от него может зависеть живучесть систем, жизнь, благосостояние групп или коллективов людей. Как достичь максимального эффекта в условиях решения конкретной задачи, которых может быть довольно большое множество? Это зависит от ряда факторов и целевых установок, которые могут ставиться при решении задач. В целом охватить данную проблематику достаточно затруднительно. Поэтому мы будем ставить и пытаться решить сначала довольно простую, даже элементарную задачу.

Прежде всего, следует отметить некоторые наиболее важные компоненты частей данных систем. В частности, что понимать под состоянием элементов и целых систем, от каких факторов и компонентов они зависят и т.д. Это проще всего рассматривать в пространстве-среде конкретной системы. И заранее следует указать на множество трудностей, которые могут встречаться при построении количественных моделей систем.

Целью данной статьи является предложить простейшую математическую модель для оценивания отрицательного влияния человеческого фактора при управлении технической системой и дать некоторые рекомендации по его уменьшению.

Элементарная модель

Область программного прогноза. Создаётся сложная техническая система для выполнения некоторого предусмотренного задания в течение требуемого времени. Априорно оценивается и обеспечивается величина заданного показателя качества в течение этого времени работы системы. Допускается возможность возникновения наиболее вероятной нештатной ситуации в процессе её работы. Предполагается, что в случае её возникновения управляющий системой человек (звено) в течение некоторого времени сможет устранить неисправность в системе, и она продолжит дальнейшую работу. Для этой цели человек до начала применения системы по назначению должен быть заранее обучен устранению нештатной ситуации. Спрашивается сколько времени надо предусмотреть для устранения возможной нештатной ситуации?

Для решения данной задачи воспользуемся математической моделью J. Musa[1], предложенной им при оценивании надёжности программного обеспечения, которое предварительно до использования по назначению в течение некоторого времени проходило тестирование с целью определения и устранения возникающих в нём ошибок.

При условии, что в работе справедлив экспоненциальный закон безотказности, то есть когда приработка и старение программного обеспечения исключены, имеет место следующее выражение для вероятности безотказной работоспособности программного обеспечения:

$$P(t,\tau) = e^{-\frac{t}{T_0} e^{-\frac{\tau}{E_0 T_0}}}, \qquad (1)$$

где t,τ – времена непрерывной работы по назначению и тестирования программы, T_0 – среднее время безотказной работы при $\tau = 0$, E_0 – начальное число ошибок в программе.

При произвольных распределениях времён можно записать [2]:

$$P(t,\tau) = e^{-\int_0^t \lambda(z)dz\, e^{-\int_0^\tau \nu(\theta)d\theta}}, \qquad (2)$$

где $\lambda(t)$ – интенсивность отказа, а $\nu(\tau)$ – интенсивность тестирования программы. А пользуясь определением ресурса надёжности Н. М. Сидякина [3], (2) представим в виде:

$$P(r(t), b(\tau)) = e^{-r(t)\, e^{-b(\tau)}}. \qquad (3)$$

В дальнейшем условно будем называть $r(t)$ ресурсом расхода надёжности системы, а $b(t)$ – ресурсом восстановления работоспособности системы.

В рамках поставленного вопроса в данном разделе – сколько времени надо предусмотреть для устранения возможной нештатной ситуации – сначала решим вспомогательный пример. Цель примера – показать, как связаны графически оба введённых ресурса.

Пример 1. Пусть вероятность выполнения задания системой задана в виде:

$$P(r,b) = e^{-re^{-b}}, \qquad (4)$$

где r, b – ресурсы расхода и восполнения работоспособности системы, представим их и вероятность в дискретном виде:

$$r_i = 1,2\ldots5;\ b_j = 1,2\ldots5;\ P_{i,j} = e^{-r_i e^{-b_j}}. \qquad (5)$$

На рис. 1 и 2 представлены графическая и матричная зависимости на диагонали от левого верхнего угла к правому нижнему углу, построена кривая вероятностей в зависимости от номеров в порядке их возрастания от 1 до 5. Представим подробнее построение этой кривой на основе алгоритма линейной интерполяции [4]:

$$A(t)=linterp(x,y,t). \qquad (6)$$

Для условий нашего примера запишем транспонированные координаты переменных по осям *r, P*:

$$r(1,2,3,4,5)^T;\ P(0.692, 0.763, 0.861, 0.929, 0.967)^T. \qquad (7)$$

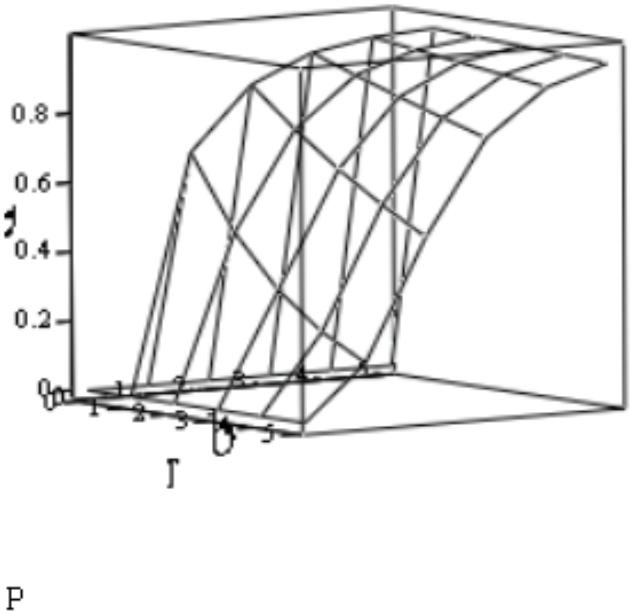

Рис. 1..

$$P := \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.692 & 0.873 & 0.951 & 0.982 & 0.993 \\ 0 & 0.479 & 0.763 & 0.905 & 0.964 & 0.987 \\ 0 & 0.332 & 0.666 & 0.861 & 0.947 & 0.98 \\ 0 & 0.23 & 0.582 & 0.819 & 0.929 & 0.973 \\ 0 & 0.159 & 0.508 & 0.78 & 0.912 & 0.967 \end{pmatrix}$$

Рис. 2.

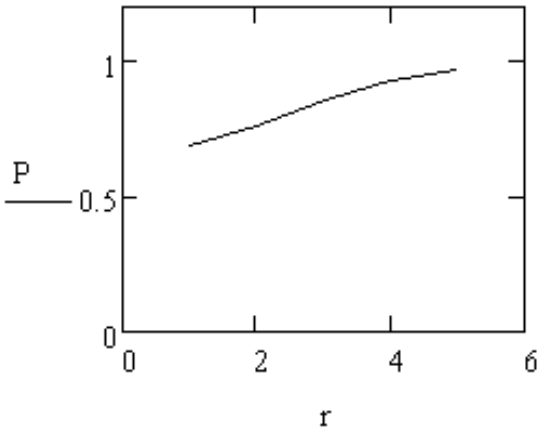

Рис. 3.

Зависимость (7) представлена на рисунке (3).

Из рис. 3 следует, что независимо от того, что величина ресурса r надёжности увеличивается (смещение вниз таблицы) значения вероятностей P на указанной диагонали возрастают. Это возрастание обуславливается тем, что с увеличением величины ресурса восстановления b значение экспоненты в показателе вероятности уменьшается, а сама вероятность P возрастает и при $b \to \infty$ будет стремиться к единице. Но следует иметь в виду то, что восстановление должно производиться перед началом применения системы по назначению.

Теперь предположим, что система начинает подвергаться испытаниям до начала использования. Проводится ряд испытаний с целью выявления и устранения возникающих неисправностей, которые в будущем могут нарушать процесс штатной её эксплуатации. При этом предварительные испытания должны проводиться до тех пор, пока не будет возможным построить с достаточной точностью закон распределения восстановления возникающих неисправностей. Благодаря этому человек по управлению приобретёт достаточно прочные навыки по оперативному устранению нештатных ситуаций в процессе эксплуатации системы.

Поясним ещё раз, но более детально смысл формулы J. Musa, представленной в виде формулы (4). Обратим внимание на то, что оба ресурса в этой формуле вводятся одинаково и ступенчато. Цифры вероятностей первой

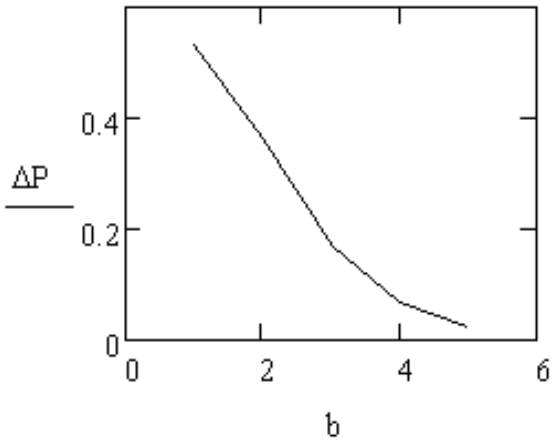

Рис. 4.

колонки матрицы на рис. 2 по мере увеличения ресурса r (расхода надёжности) при единичном значении ресурса $b = 1$ (ресурса восстановления) монотонно уменьшаются от 0.692 до 0.159. Если $b = 2$ для второй колонки матрицы, то падение вероятностей будет менее значительным, а именно от 0.873 до 0.508. Если ввести ещё одну единицу ресурса, то есть $b = 3$, то уменьшение вероятности станет ещё менее значительным, а именно от 0.951 до 0.780. И наконец, для граничного значения столбца 5, когда $b = 5$, уменьшение вероятности становится самым низким, а именно от 0.993 до 0.967. Это показывает насколько велико значение раннего, проводимого до начала эксплуатации, эффекта предварительного восстановления системы. На этом заканчивается изложение примера.

На рис. 4 дополнительно показано абсолютное постолбцовое уменьшение вероятности действия системы при заданных значениях $r, b = 5$:

$$b = (1,2,3,4,5)^T,\ \Delta P = (0.533, 0.365, 0.171, 0.070, 0.026)^T.$$

Итак, на абстрактном конкретном числовом примере мы детально рассмотрели поведение вероятности функционирования системы, описываемой математической моделью J. Musa. Однако мы сознательно изменили предложенную им область приложения к оцениванию надёжности программного обеспечения с учётом его предварительного тестирования и исправления обнаруженных в нём ошибок. Мы гипотетически заменили область приложения другой областью. Предполагая до начала работы системы в будущем, что в ней возникнет нештатная ситуация, могущая изменить траекторию движения, но эта ситуация звеном управления будет исправлена, а система войдёт снова в нормальный режим.

Функционирование системы с одной нештатной ситуацией. До начала применения системы предполагается выполненным безошибочное априорное оценивание её работы в течение времени t:

$$P(t) = e^{-\int_0^t \lambda(z)dz}, \qquad (8)$$

то есть величина ресурса $r(t)=\int_0^t \lambda(z)dz$ известна, но на интервале $[0,t]$ может случайно возникнуть нештатная ситуация, которая может в дальнейшем нарушить нормальное поведение системы. Предположим, что закон распределения времени возникновения этой ситуации известен. Зададим его:

$$H(y)=1-e^{-\int_0^y \nu(z)dz}, \quad 0\le y\le t. \tag{9}$$

Допустимое время выхода из нештатной ситуации определяется законом:

$$B(\theta)=1-e^{-\int_0^\theta \mu(z)dz}, 0\le\theta\le d. \tag{10}$$

Этот закон распределения должен быть установлен в результате предварительного обучения устранению нештатной ситуации управляющим звеном до применения системы.

В простейшем случае предположим, что закон (10) не зависит от времени возникновения ситуации в работе системы при эксплуатации. Тогда ресурс устранения ситуации будет равен:

$$b(\theta)=\int_0^\theta \mu(z)dz, \tag{11}$$

а вероятность выполнения задания системой

$$P(r(t,b(d))\approx e^{-r(t+d)}e^{-b(d)}. \tag{12}$$

В общем случае, когда нештатная ситуация происходит в момент времени y и продолжительность её устранения связана с этим моментом, тогда

$$b(\theta,y)\approx \int_0^{\theta(y)} \mu(y)dy, 0\le\theta(y)\le d(y), \tag{13}$$

и, соответственно, вероятность выполнения задания системой станет более сложной:

$$P(r(t,b(d(y)))\approx e^{-r(t+d(y))}e^{-b(d(y))}. \tag{14}$$

Знак $\approx$ применён для того, чтобы при записи избежать использования операции интегрирования.

Если в процессе функционирования системы предусматривается более одной нештатной ситуации, тогда алгоритм вычисления вероятности значительно усложнится. В отдельных случаях, на наш взгляд, может применяться имитационное моделирование для решения задачи.

Пример 2. Безотказность управляемой технической системы характеризуется следующими значениями численных параметров: время непрерывной работы составляет $10h.$, априорно определённое распределение времени до отказа задано нормальной плотностью вероятности $f(t)=dnorm(m,\sigma,t), m=100h., \sigma=12\text{h}.$, поэтому вероятность её безотказной работы составляет $P(10)=0,993$. На ней может возникнуть одна нештатная программная ситуация, приводящая к нарушению работоспособности системы. Распределение нарушения происходит по экспоненциальному закону с интенсивностью $\lambda=0.2h^{-1}$, средняя величина ресурса надёжности составит $r=2h.$,а значение первой экспоненты в формуле J.Musa будет равно $e^{-2}=0.135$. Для того, чтобы сохранить работоспособность технической системы на уровне $P(10)=0,993$ после устранения нештатной ситуации потребуется следующее значение ресурса восстановления $b=9.903$с вероятностью $0,9999$, которая подбирается опытно для постановки и получения в результате решения уравнения $e^{-2e^{-b}}-0,9999=0$.

Численная реализация этого алгоритма, даже сравнительно несложного в своей структуре, потребует приложения достаточно значительных усилий. Поэтому для иллюстрации вероятностных расчётов рассмотрим прикладной пример с применением другого алгоритма.

Спрашивается, сколько испытаний предварительно надо произвести для подтверждения этой вероятности и какое время затратить, если на один прогон программы требуется $\tau=0.005h$. Итак, вероятность отсутствия ошибки $p=0,9999$, а вероятность ошибки $q=0,0001$. Среднее число ошибок в n испытаниях равно np, а среднеквадратическое отклонение – $\sqrt{npq}$, поэтому плотность вероятности числа испытаний представим $g(x)=\frac{C}{\sqrt{2\pi npq}}e^{-\frac{(x-np)^2}{2npq}}, C=1,852$. Данная плотность превращается в дельта-функцию при $n=100$. Поэтому время испытаний становится равным $n\tau$. Если за время функционирования системы $10h.$ произойдёт одна нештатная ситуация, то время испытаний составит $0,5h.$Вероятность выполнения задания системой сохранится прежней, то есть равной $P=P(10)\mathrm{e}^{-2e^{-b}}=0,993$.

Если же в системе ожидается 10 нештатных ситуаций, тогда вероятность выполнения задания системой становится равной $P=P(10)e^{-2e^{-0.99}}=0.472$. Это означает, что предварительных испытаний программного обеспечения по устранению нештатных испытаний было выполнено недостаточно, так как вероятность исправной работы системы меньше расчётной $P<0.993$.

Дискретное представление ресурса. В теории надёжности рассматривается непрерывное представление ресурса $r(t)=\int_0^t \lambda(z)dz=-\ln P(t)$. Ресурс понимается в смысле профессора Н. М. Седякина. При испытаниях программного обеспечения приходится использовать не непрерывное время, а время, представляемое в дискретном виде, а именно в количестве прогонов программы. Поэтому имеет смысл выражать ресурс

в зависимости от числа прогонов программы. Предложим модель ресурса, зависящего от числа прогонов. Сначала запишем выражение для вероятности безотказной работы для непрерывного времени испытаний:

$$P(t) = \frac{N_0 - n(t)}{N_0}, \qquad (15)$$

где N_0 – количество объектов, первоначально поставленных на испытание, $n(t)$ – количество объектов, отказавших за время испытаний t.

Представим, что время t представлено дискретно $t = m\tau$, где τ – время одного кванта (дискрета), а m – полное число квантов за время до отказа. Первоначальное число объектов представим в виде n_0. Тогда

$$P(n_0\tau) = \frac{n_0\tau - m\tau}{n_0\tau} = 1 - \frac{m}{n_0}. \qquad (16)$$

Далее предположим, что формула (16) верна лишь для некоторого времени t_i, $i = 1,2,\ldots, t_{i+1} > t_i$, для всех i. Поэтому (16) можно представить в виде

$$P(t_i) = 1 - \frac{m_i}{n_i}(t_i),$$

а величину дискретного ресурса –

$$r_i(t_i) = -\ln[1 - \frac{m_i}{n_i}(t_i)]. \qquad (17)$$

Это касается только ресурсов для формулы J. Musa (($r_i(t_i), b_i(t_i)$ программного обеспечения), но не относится к ресурсу аппаратуры с непрерывным временем её функционирования. Расчёт безошибочности работы системы выполняется так же, как было выше указано.

Замечание о распределении требований, предъявляемых к технической системе и человеческому звену управления. В том случае, если к системе предъявляются особые требования, а не только просто вероятность выполнения ею задания, (например, безопасность экипажа, величина ущерба и риска и другие), то необходимо учитывать ряд дополнительных системных параметров. С учётом значений этих параметров необходимо скорректировать предлагаемую модель с целью выполнения экстремальных решений известными методами для получения желаемого результата.

Заключение

В статье предложена модель для снижения влияния нештатных ситуаций при функционировании сложной системы. Ликвидация этих нештатных ситуаций осуществляется силами человеческого управляющего звена. Для увеличения эффекта ликвидации звено управления должно предварительно до применения системы по назначению обучаться в лабораторных условиях. При этом выполняется имитация и необходимый мониторинг исходных данных для ликвидации ситуации в работе системы.

В качестве математической модели предложено использовать модель J. Musa, применяемой при тестировании программного обеспечения. Предлагается алгоритм для определения необходимого ресурса восстановления нештатной ситуации. Характеристики алгоритма служат руководством при ликвидации нештатной ситуации. Приводятся элементарные примеры численных расчётов для данной эвристической модели. Формулируются некоторые рекомендации по практической реализации предлагаемой модели.

Ограничительным моментом модели является то, что её нецелесообразно применять к комплексу «техника и программное обеспечение». Это объясняется тем, что математическая модель J. Musa не разработана применительно к проведению доработок по устранению отказов и неисправностей в частности, а тем более в совокупности с ошибками программного обеспечения.

Литература

1. Musa, J. A theory of software reliability and its application / J. Musa // IEEE Trans. on software Eng. – Sept. 1975. – Vol. SE-1 – P. 312–327.

2. Смагин, В. А. Дискретный аналог математической модели J. Musa и рекомендации по его применению в исследовании безошибочной работы коллективов и надёжности программного обеспечения / В.А. Смагин // Труды ВКА имени А. Ф. Можайского. – 2007. – Вып. 621. – 163 с.

3. Седякин, Н. М. Об одном физическом принципе теории надёжности / Н.М. Седякин // Изв. АН СССР. Техническая кибернетика. – 1966. – № 3. – С. 80–87.

4. Кирьянов, Д. В. Mathcad 12 / Д.В. Кирьянов. – СПб.: БХВ-Петербург, 2005 – 576 с.