ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 19 **МАТЕМАТИКИ** **Выпуск 2,3**
2012

В. А. Каштанов, **О. Б. Зайцева** (Москва, МИЭМ НИУ ВШЭ, АГПА)**. О минимакных подходах в задачах безопасности.**

Связь проблем надежности и безопасности была очевидна специалистам давно. При низких характеристиках надежности (безотказности и ремонтопригодности) нельзя обеспечить высокую безопасность функционирования различных технических систем. Примером могут служить транспортные системы, энергетические системы, вычислительные системы и т. п. В ряде работ исследовалась зависимость показателей безопасности от характеристик надежности и стратегии технического обслуживания, поддерживающей систему в работоспособном состоянии [3–6]. При построении таких математических моделей учитывались такие характерные особенности ситуации, как наличие противоборствующих сторон, случайный характер возникновения отказов, наличие управления (управляющих воздействий), позволяющего улучшать показатели безопасности, ставить и решать оптимизационную задачу. При построении случайного процесса, описывающего эволюцию системы, и постановке задачи оптимизации предполагается, что характеристики надежности известны. Однако на практике дело обстоит не так. Оценки характеристик надежности получаются в результате статистических испытаний и точно не известны. Следовательно, точно не известны вероятностные характеристики случайного процесса, описывающего эволюцию исследуемой системы, которым мы управляем и от поведения которого зависят показатели безопасности. Поэтому в реальной ситуации управлять приходится по неполным данным, что меняет постановку математической задачи.

В настоящей работе мы исследуем известную модель [1, 2] технического обслуживания в условиях неполной информации для анализа показателей безопасности.

Процесс атак на систему защиты. Попытки пройти систему защиты осуществляются периодически. Предполагаем, что этот процесс описывается процессом Пуассона с параметром λ.

Процесс функционирования технической системы. Пусть задана система, у которой время безотказной работы распределено по закону $F(x) = \mathbf{P}\{\xi < x\}$, $\overline{F}(x) = 1-F(x) = \mathbf{P}\{\xi \geqslant x\}$. Предположим, что появившийся при функционировании системы отказ самостоятельно обнаруживается (проявляется) мгновенно.

В начальный момент $t_0 = 0$ начинается эксплуатация системы защиты и назначается плановое предупредительное обновление (профилактика) системы через время $v \geqslant 0$, распределенное по закону $G(x) = \mathbf{P}\{v < x\}$, $G(0) = 0$.

Назначение плановых предупредительных обновлений системы через случайное время $v \geqslant 0$ означает введение рандомизации в процесс принятия решений, т. е. в тот момент, когда нужно принимать решение, строится реализация τ случайной величины v, $\{v = \tau\}$, распределенной по закону $G(x)$, и плановое предупредительное обновление системы проводится через время τ.

Если к назначенному моменту $v \geqslant 0$ система не отказала (произошло событие $\{v < \xi\}$), то в момент $v \geqslant 0$ начинается плановое предупредительное обновление системы, которое по предположению полностью обновляет систему. Обозначим

длительность этого планового предупредительного (профилактического) обновления γ_1, а $F_1(x) = \mathbf{P}\{\gamma_1 < x\}$ обозначим функцию распределения этой длительности, $\overline{F}_1(x) = \mathbf{P}\{\gamma_1 \geqslant x\}$.

Наконец, если отказ системы наступил до назначенного момента $v \geqslant 0$ (произошло событие $\{v \geqslant \xi\}$), то в момент обнаружения отказа ξ начинается внеплановое аварийное обновление системы. Длительность этой восстановительной работы обозначим γ_2, а закон распределения обозначим $F_2(x) = \mathbf{P}\{\gamma_2 < x\}$, $\overline{F}_2(x) = \mathbf{P}\{\gamma_2 > \xi\}$.

После проведения возможных восстановительных работ, когда по предположению система полностью обновляется, осуществляется перепланирование момента проведения следующей предупредительной восстановительной работы независимо от прошлого течения процесса и весь процесс обслуживания повторяется заново.

Построение функционала (*показателя безопасности*). Для описанной модели функционирования системы защиты и процесса атак в [3] получены зависимости математического ожидания времени до катастрофы (момента преодоления системы защиты) от исходных характеристик. Если обозначить $\mathbf{E}_0(G)$ математическое ожидание времени до катастрофы при условии, что в начальный момент система исправна, то

$$\mathbf{E}_0(G) = \left[\int_0^\infty \left[\int_0^u \overline{F}(y)\,dy + \overline{F}(u)\int_0^\infty e^{-\lambda t}F_1(t)\,dt + F(u)\int_0^\infty e^{-\lambda t}\overline{F}_2(t)\,dt\right] dG(u)\right] \times\left[\int_0^\infty \left[1 - \overline{F}(u)\int_0^\infty e^{-\lambda t}\,dF_1(t) - F(u)\int_0^\infty e^{-\lambda t}\,dF_2(t)\right] dG(u)\right]^{-1}. \quad (1)$$

Величины $\alpha_i = \int_0^\infty e^{-\lambda t}\,dF_i(t)$, $i = 1, 2$, определяют вероятность того, что во время восстановительной работы i-го вида не произойдет катастрофы. Естественно считать $\alpha_1 \geqslant \alpha_2$, так как аварийный ремонт длится дольше предупредительного.

Тогда $\int_0^\infty e^{-\lambda t}\overline{F}_i(t)\,dt = (1 - \alpha_i)/\lambda$ и из (1) получаем

$$\begin{aligned}\mathbf{E}_0(F, G) &= \left[\int_0^\infty \left[\lambda\int_0^u \overline{F}(y)\,dy + (1 - \alpha_1) - (\alpha_2 - \alpha_1)\int_0^u dF(y)\right] dG(u)\right] \\ &\quad\times\left[\lambda\int_0^\infty \left[1 - \alpha_1 - (\alpha_2 - \alpha_1)\int_0^u dF(y)\right] dG(u)\right]^{-1} \\ &= \int_0^\infty\int_0^\infty \min\{y, u\}\,dF(y)\,dG(u)\Big/\int_0^\infty\int_0^\infty B(y, u)\,dF(y)\,dG(u) + \frac{1}{\lambda}, \quad (2)\end{aligned}$$

где

$$B(y, u) = (1 - \alpha_2)I\{y \leqslant u\} + (1 - \alpha_1)I\{y > u\} = \begin{cases} 1 - \alpha_2, & y \leqslant u, \\ 1 - \alpha_1, & y > u. \end{cases} \quad (3)$$

Равенство (2) показывает, что математическое ожидание $\mathbf{E}_0(F, G)$ есть дробно-линейный функционал относительно распределения G, определяющего периодичность проведения плановых восстановительных работ, и распределения F времени безотказной работы.

Постановка минимаксной задачи. Так как характеристики времени безотказной работы определяются по результатам статистических испытаний и после их обработки получают оценки этих характеристик, то считаем, что функция распределения времени известна не точно, а известно множество распределений W, которому она принадлежит, $F \in W$. Если обозначить Ω множество распределений положительных случайных величин, то задачу можно сформулировать так: определить

$$\max_{G\in\Omega}\ \inf_{F\in W} \mathbf{E}_0(F, G) = \mathbf{E}_0(F_0, G_0) \quad (4)$$

и распределения F_0, G_0) ,на которых этот максимин достигается.

Решение. Математическое ожидание времени до катастрофы есть дробно-линейный функционал (2). При поиске внутреннего экстремума воспользуемся утверждением [1]: *если* $A(y, u)$ *— неубывающая функция по переменной* y *при любом* u, *а*

$B(y,u)$ — невозрастающая функция по переменной y при любом u, то при любом распределении G справедливо неравенство

$$I(\Phi_1,G) = \int_0^\infty\int_0^\infty A(y,u)\,d\Phi_1(y)\,dG(u)\Big/\int_0^\infty\int_0^\infty B(y,u)\,d\Phi_1(y)\,dG(u)$$
$$\geqslant \int_0^\infty\int_0^\infty A(y,u)\,d\Phi_2(y)\,dG(u)\Big/\int_0^\infty\int_0^\infty B(y,u)\,d\Phi_2(y)\,dG(u) = I(\Phi_2,G),$$

функция $\Phi_2(y)$ мажорирует функцию Φ_1: $\Phi_2(y)\geqslant\Phi_1(y)$.

Если существует распределение F_0, мажорирующее любое распределение $F\in W$, $F_0\geqslant F$, то $I(F_0,G)\leqslant I(F,G)$. Функционал $I(F_0,G)$ дробно-линейный относительно распределений $G\in\Omega$. Поэтому если максимум этого функционала существует, то оптимальную стратегию управления можно искать в классе детерминированных стратегий $\Omega^{(0)}$ [1]:

$$G(x)=0,\quad \text{если}\quad x\leqslant u,\quad G(x)=1,\quad \text{если}\quad x>u. \tag{5}$$

Таким образом, получаем оценку

$$\max_{G\in\Omega}\inf_{F\in W} I(F,G)\geqslant \max_{G\in\Omega^{(0)}} I(F_0,G). \tag{6}$$

З а м е ч а н и е. Если $F_0\in W$, то улучшить оценку нельзя,

$$\max_{G\in\Omega}\min_{F\in W} I(F,G)=\max_{G\in\Omega^{(0)}} I(F_0,G).$$

Приведем два примера. Для функционала (2) условия выше приведенного утверждения выполняются.

Пусть $W=\Omega\{n,\overline{y},\overline{\pi}\}$ есть множество распределений, которые в заданных точках $\overline{y}$ принимают заданные значения $\overline{\pi}$ [1]. В этом пространстве существует мажорирующее распределение $F_0(y)=\pi_k$, $y_{k-1}<y\leqslant y_k$, $0<k\leqslant n+1$.

Следовательно,

$$\mathbf{E}_0(F_0,G_0) = \max_{G\in\Omega}\min_{F\in W}\mathbf{E}_0(F,G)=\max_{G\in\Omega}\mathbf{E}_0(F_0,G)$$
$$= \max_{x\in[0,\infty)}\left\{\left[\sum_{k=0}^{n}\min\{x,y_k\}(\pi_{k+1}-\pi_k)\right]\Big/\left[\sum_{k=0}^{n}B(x,y_k)(\pi_{k+1}-\pi_k)\right]\right\}+\frac{1}{\lambda}$$
$$= \left[\sum_{k=0}^{n}\min\{x_0,y_k\}(\pi_{k+1}-\pi_k)\right]\Big/\left[\sum_{k=0}^{n}B(x_0,y_k)(\pi_{k+1}-\pi_k)\right]+\frac{1}{\lambda}. \tag{7}$$

Профилактики надо проводить через время x_0, и равенство (7) дает значение гарантированного уровня безопасности в этих условиях неопределенности.

Пусть $W=\Omega(\mu)$ есть множество распределений с фиксированным математическим ожиданием μ, $\Omega(\mu)=\{F:\ \mu=\int_0^\infty[1-F(x)]\,dx\}$. Для технических систем естественно считать, что распределение стареющее. Тогда известно [2], что существует распределение $F_0(x)$, равное $1-e^{-x/\mu}$ при $0\leqslant x\leqslant\mu$, и равное 1 при $x>\mu$, которое мажорирует распределения множества $\Omega(\mu)$.

Следовательно,

$$\mathbf{E}_0(F_0,G_0) = \max_{G\in\Omega}\mathbf{E}_0(F_),G)=\max_{u\geqslant 0}\left\{\frac{1}{\lambda}+\frac{[\mu(1-e^{\min\{u,\mu\}/\mu})]}{(1-\alpha_1)-(\alpha_2-\alpha_1)F_0(u)}\right\}$$
$$= \frac{1}{\lambda}+\frac{[\mu(1-e^{-1})]}{(1-\alpha_1)-(\alpha_2-\alpha_1)(1-e^{-1})}$$

и достигается этот максимум при $u_0=\mu=0$.

СПИСОК ЛИТЕРАТУРЫ

1. *Барзилович Е. Ю.*, *Каштанов В. А.* Организация обслуживания при ограниченной информации о надежности системы. М.: Советское радио, 1975.
2. *Барлоу Р.*, *Прошан Ф.* Математическая теория надежности. М.: Советское радио, 1969, 357 с.
3. *Зайцева О. Б.* Анализ полумарковской модели безопасности. — Обозрение прикл. и промышл. матем., 2011, т. 18, в. 2, с. 223–235.
4. *Злотов А. В.*, *Ливанов Ю. В.*, *Хачатуров В. Р.* Методика и компьютерные модели проектирования с учетом надежности и безопасности объектов и коммуникаций инфраструктуры региона. — В сб.: Фундаментальные проблемы системной безопасности и устойчивости, ВЦ РАН. М.: Вузовская книга, 2011, в. 3, с. 77–86.
5. *Ильичев А. В.*, *Северцев Н. А.* Определение показателей эффективности и безопасности. — В сб.: Фундаментальные проблемы системной безопасности и устойчивости, ВЦ РАН. М.: Вузовская книга, 2011, в. 3, с. 27–37.
6. *Каштанов В. А.*, *Зайцева О. Б.* О методологии построения математических моделей безопасности. — В сб.: Фундаментальные проблемы системной безопасности и устойчивости, ВЦ РАН. М.: Вузовская книга, 2011, в. 3, с. 151–158.