

БЕЗОПАСНОСТЬ И НАДЕЖНОСТЬ СИСТЕМЫ ЗАЩИТЫ ОБЪЕКТА

А. В. Бецков

Рассмотрим особо важную стационарную систему как объект защиты (ОЗ), имеющий систему безопасности (СБ). Полагаем, что в каждый момент времени объект защиты может находиться в одном из двух состояний: работоспособном или отказа, а система безопасности в одном из трех состояний: работоспособном, ложного отказа (ложное срабатывание) или опасного отказа (несрабатывание). Предполагается, что при ложном отказе СБ или в случае отказа ОЗ при исправной СБ система немедленно выводится в состояние безопасного останова. Отказ ОЗ при опасном отказе СБ считается недопустимым событием (авария, ЧП). Таким образом, в каждый момент времени система может находиться в одном из следующих состояний:

- БФ – безопасное функционирование (работоспособный ОЗ, при работоспособной СБ);
- БОс – безопасный останов вследствие отказа ОЗ при работоспособном СБ (предотвращение ЧП);
- БОт – безопасный останов из-за ложного отказа СБ;
- ОФ – опасное функционирование (функционирование ОЗ при опасном отказе СБ).

В такой постановке для исследуемой системы можно построить граф состояний и переходов полумарковской модели процесса функционирования системы (рис. 1).

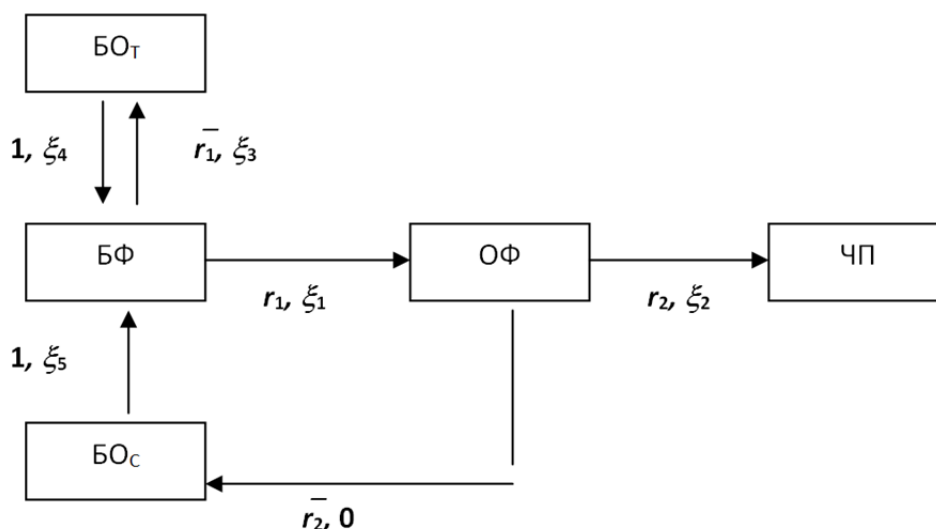


Рис. 1. Граф состояний и переходов функционирования системы:
 r_i – вероятность перехода; $\bar{r}_i = 1 - r_i$; ξ – случайное время до перехода в i -состояние

Обозначим элементарные (первичные) события системы: a – отказ ОЗ; b – ложный отказ СБ; c – опасный отказ СБ. Далее эти обозначения мы будем использовать для случайных наработок элементов до наступления соответствующих событий.

Случайные наработки a , b , c считаем независимыми, а их функции распределения будут $F_a(t)$, $F_b(t)$, $F_c(t)$. Будем полагать, что состояние СБ соответствует тому из событий b , c , которое наступило раньше, например, в случае $b \leq c$ считается, что СБ находится в состоянии ложного отказа.

Для ведения исследований по полумарковской модели (см. рис. 1) необходимо определить вероятности r_1 , r_2 , а также средние времена пребывания в состоянии до выхода из них. Для этого

предположим, что восстановление после безопасных остановов не происходит. Граф состояний и переходов для этого случая можно представить в следующем виде (рис. 2).

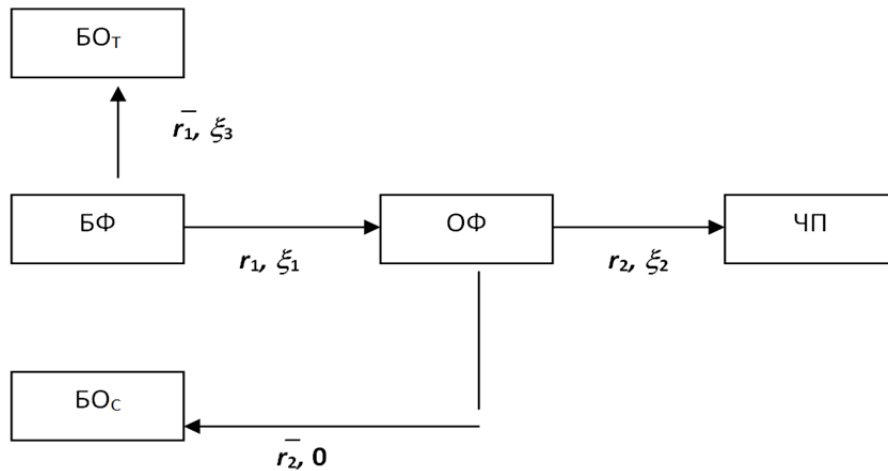
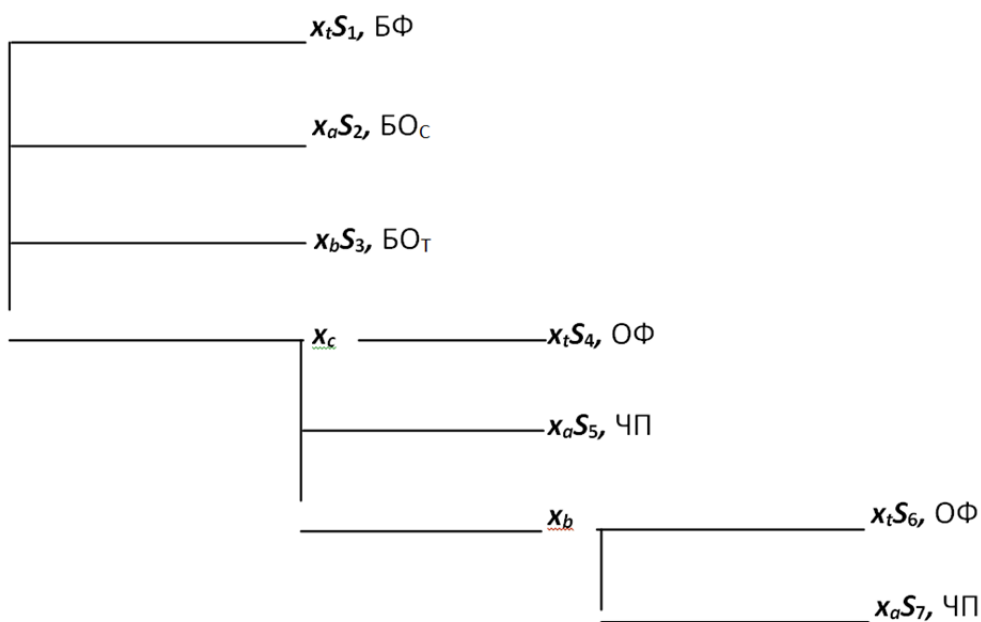


Рис. 2. Граф состояний и переходов полумарковской модели

Здесь ОЗ – СБ в отсутствии восстановления после остановов и отказов.

Состояние системы в некоторый момент t будем описывать многозначной логической (индикаторной) переменной $Q \in \Omega = \{\text{БО}_T, \text{БО}_C, \text{ОФ}, \text{ЧП}\}$. В момент времени t происходит некоторое событие. Состояние системы в момент времени t зависит от порядка наступления элементарных событий a, b, c, t . Для описания зависимости Q от порядка наступления элементарных событий используем последовательное дерево событий [1]. В последовательном дереве событий ставятся элементарные события так, что любому пути из корневой вершины v_0 в некоторую вершину v , а значит, и к самой вершине v , однозначно соответствует некоторая последовательность элементарных событий в порядке их наступления, которой, в свою очередь, соответствует некоторое состояние системы – $Q(v)$ из множества $\Omega \cup z$, где z означает «состояние не определено». В усеченном (редуцированном) последовательном дереве событий «висячими» («листьями») являются такие вершины, для которых $Q(v) \neq z$, и все их потомки в полном последовательном дереве событий также имеют значение $Q(v)$ [2]. Усеченное последовательное дерево событий для исследуемой системы можно представить на рис. 3.



«Листьям» усеченного последовательного дерева событий соответствуют сложные события, т.е. множества последовательностей элементарных событий, которые обозначим $S_1 - S_7$:

$$S_1 = \{t \leq a, t \leq b, t \leq c\}, S_2 = \{a \leq t, a \leq b, a \leq c\}, S_3 = \{b \leq t, b \leq a, b \leq c\}, S_4 = \{c \leq t, t \leq a, t \leq b\},$$

$$S_5 = \{c \leq a, a \leq b, a \leq b\}, S_6 = \{c \leq b \leq t \leq a\}, S_7 = \{c \leq b \leq a \leq t\}.$$

Зная распределение случайных величин a, b, c , вероятности событий $S_1 - S_7$ можно определить следующим образом.

Обозначим $P_1 = P\{S_1\}, i = \overline{1, 7}, \bar{F} = 1 - F$.

Тогда

$$P_1 = \bar{F}_a(t) \otimes \bar{F}_b(t) \otimes \bar{F}_c(t); P_2 = \int_0^t \bar{F}_b(x) \otimes \bar{F}_c(x) dF_a(t);$$

$$P_3 = \int_0^t \bar{F}_a(x) \otimes \bar{F}_c(x) dF_b(t); P_4 = F_c(t) \otimes \bar{F}_a(t) \otimes F_b(t);$$

$$P_5 = \int_0^t F_c(x) \otimes \bar{F}_b(x) dF_a(x); P_6 = \bar{F}_a(t) \otimes \int_0^t F_c(x) dF_b(x);$$

$$P_7 = \int_0^t \int_0^x F_c(y) dF_b(y) dF_a(y), \quad (1)$$

где \otimes – знак Кронекерского умножения.

Как видно из (1), вероятности $P_i = P\{S_i\}, i = \overline{1, 7}$ являются функциями времени $P_i(t), i = \overline{1, 7}$. В силу несовместимости $S_1 - S_7$ (см. рис. 1) можно определить вероятности состояний системы:

$$P_{\text{БФ}}(t) = P\{Q(t) = \text{БФ}\} = P_1(t);$$

$$P_{\text{БО}_C}(t) = P\{Q(t) = \text{БО}_C\} = P_2(t);$$

$$P_{\text{БО}_T}(t) = P\{Q(t) = \text{БО}_T\} = P_3(t);$$

$$P_{\text{ОФ}}(t) = P\{Q(t) = \text{ОФ}\} = P_4(t) + P_6(t);$$

$$P_{\text{ЧП}}(t) = P\{Q(t) = \text{ЧП}\} = P_5(t) + P_7(t). \quad (2)$$

Зная вероятности состояний системы (2) для случая отсутствия восстановления после опасных остановов (см. рис. 1), можно определить вероятности r_1, r_2 . Обозначим $P(\infty) = \lim_{t \rightarrow \infty} P(t)$.

В соответствии с рис. 1 имеем

$$P_{\text{БО}_T}(\infty) = \bar{r}_1 = 1 - r_1; P_{\text{БО}_C}(\infty) = r_1 \times \bar{r}_2 = r_1 \times (1 - r_2);$$

$$P_{\text{ЧП}}(\infty) = r_2 \times r_1.$$

Откуда

$$r_1 = 1 - P_{\text{БО}_T}(\infty), r_2 = 1 - P_{\text{БО}_C}(\infty) / r_1. \quad (3)$$

Тогда представляется возможным определить распределение случайных величин ξ_1 и ξ_2 , $\xi_1 + \xi_2$:

$$F_{\xi_1}(t) = P_{\text{БО}_T}(t) / P_{\text{БО}_T}(\infty); F_{\xi_2}(t) = P_{\text{БО}_C}(t) / P_{\text{БО}_C}(\infty). \quad (4)$$

Пользуясь (4), найдем $M\xi_1, M\xi_2, M\xi_3$:

$$M\xi_1 = \int_0^\infty F_{\xi_1}(t) dt; M\xi_2 = \int_0^\infty \bar{F}_{\xi_1 + \xi_2}(t) dt - M\xi_1;$$

$$M\xi_1 = \int_0^{\infty} \bar{F}_{\xi_1}(t) dt. \quad (5)$$

Здесь $\bar{F}(t) = 1 - F(t)$.

При известных вероятностях (2) и математических ожиданиях (5) можно определить средние времена пребывания в невозвратных состояниях системы до выхода из них (для модели рис. 1):

$$T_{\text{БФ}} = \int_0^{\infty} P_{\text{БФ}}(t) dt; \quad T_{\text{ОФ}} = r_2 \times M\xi_2. \quad (6)$$

Определив $T_{\text{БФ}}$ и $T_{\text{ОФ}}$, рассмотрим состояние (модель на рис. 3), которое учитывает восстановление системы после безопасных остановов. Запишем $T_{\text{БОС}} = M\xi_5$; $T_{\text{БОТ}} = M\xi_4$, которые означают среднее время ($T_{\text{БОС}}$ и $T_{\text{БОТ}}$) пребывания системы в состояниях БОС и БОТ соответственно.

На основании топологического метода расчета (метод топологических уравнений Мейсона [3]) можно найти формулу (выражение) для расчета среднего времени до выхода системы в ЧП $T_{\text{ЧП}}$ с учетом восстановлений после безопасных остановов [4]:

$$T_{\text{ЧП}} = T_{\text{БФ}} / (r_1, r_2) + T_{\text{ОФ}} / r_2 + \bar{r}_1 T_{\text{БОТ}} / (r_1, r_2) + \bar{r}_2 T_{\text{БОС}} / r_2. \quad (7)$$

Можно получить (определить) следующие величины:

$T_{\text{ЗФ}}^{\text{ЧП}}$ – среднее суммарное время безопасного функционирования и среднее число попаданий в состояние БФ, $n_{\text{ЗФ}}^{\text{ЧП}}$ до выхода в аварию

$$T_{\text{ЗФ}}^{\text{ЧП}} = T_{\text{БФ}} / r_1 r_2; \quad n_{\text{ЗФ}}^{\text{ЧП}} = 1 / r_1 r_2; \quad (8)$$

$T_{\text{ОФ}}^{\text{ЧП}}$ – среднее суммарное время опасного функционирования и среднее число попаданий в состояние ОФ $n_{\text{ОФ}}^{\text{ЧП}}$ до выхода в аварию:

$$T_{\text{ОФ}}^{\text{ЧП}} = T_{\text{ОФ}} / r_2; \quad n_{\text{ОФ}}^{\text{ЧП}} = 1 / r_2; \quad (9)$$

$T_{\text{ЗМТ}}^{\text{ЧП}}$ – среднее суммарное время восстановления после попадания в состояние БОС и среднее число попаданий в состояние БОС $n_{\text{ЗМС}}^{\text{ЧП}}$ до выхода в аварию:

$$T_{\text{ЗМТ}}^{\text{ЧП}} = \bar{r}_2 T_{\text{ЗМС}}^{\text{ЧП}} / r_2; \quad n_{\text{ЗМС}}^{\text{ЧП}} = \bar{r}_2 / r_2. \quad (10)$$

Заметим, что величина $n_{\text{ЗМС}}^{\text{ЧП}}$ равна среднему предотвращенных аварийных ситуаций, приходящихся на одну аварию, имеющую место, и в этом смысле является показателем *статистической безопасности*.

Введем следующие показатели оценки обеспечения безопасности функционирования системы.

1. Коэффициент опасности функционирования системы

$$k_{\text{МФ}}^{\text{ЧП}} = T_{\text{ОФ}}^{\text{ЧП}} / (T_{\text{ЗФ}}^{\text{ЧП}} + T_{\text{ОФ}}^{\text{ЧП}}). \quad (11)$$

Данный коэффициент показывает, насколько опасна работающая исследуемая система.

2. Коэффициент безопасности функционирования системы

$$k_{\text{ЗФ}}^{\text{ЧП}} = 1 - k_{\text{МФ}}^{\text{ЧП}} = T_{\text{ЗФ}}^{\text{ЧП}} / (T_{\text{ЗФ}}^{\text{ЧП}} + T_{\text{ОФ}}^{\text{ЧП}}). \quad (12)$$

Рассмотрим задачу для случая, когда наработки a, b, c имеют экспоненциальное распределение с параметрами $\lambda_a, \lambda_b, \lambda_c$. Соответственно обозначим

$$T_a = 1 / \lambda_a; \quad T_b = 1 / \lambda_b; \quad T_c = 1 / \lambda_c; \quad \lambda^* = \lambda_a + \lambda_b + \lambda_c; \quad T^* = \frac{1}{\lambda^*}.$$

Запишем следующие соотношения:

а) без учета восстановлений после безопасных остановов:

$$\begin{aligned}
 P_{\text{БФ}} &= \exp(-\lambda^* \times t); P_{\text{БО}_C} = P_{\text{БФ}} \times \lambda_a / \lambda^*; P_{\text{БО}_T} = P_{\text{БФ}} \times \lambda_b / \lambda^*; \\
 P_{\text{ОФ}} &= \exp(-\lambda_0 \times t) \times (1 - \exp(-(\lambda_b + \lambda_c) \times t) \times \lambda_c / (\lambda_b + \lambda_c)); \\
 P_{\text{ЧП}} &= (1 - \exp(-\lambda_a \times t)) \times \lambda_c / (\lambda_b + \lambda_c) - (1 - \exp(-\lambda^* \times t) \times \lambda_a \lambda_c / \lambda^* (\lambda_b + \lambda_c)); \\
 P_{\text{БО}_C}(\infty) &= \lambda_a / \lambda^*; P_{\text{БО}_T}(\infty) = \lambda_b / \lambda^*; P_{\text{ЧП}}(\infty) = \lambda_c / \lambda^*; \\
 r_1 &= (\lambda_a + \lambda_c) / \lambda^*; r_2 = \lambda_c / (\lambda_a + \lambda_c); \\
 M\xi_1 &= T^*; M\xi_2 = T_a; M\xi_3 = T^*.
 \end{aligned} \tag{13}$$

Для приближенных вычислений при $\lambda^* \times t \ll 1$ можно воспользоваться формулами

$$P_{\text{БФ}} \cong 1 - \lambda^* \times t; P_{\text{БО}_C} \approx \lambda_a \times t; P_{\text{БО}_T} \approx \lambda_b \times t, \tag{14}$$

которые получаются после разложения соответствующих вероятностей в ряд Тейлора до линейных членов и несложных преобразований. Линейная аппроксимация вероятности $P_{\text{ЧП}}(t)$ дает $P_{\text{ЧП}}(t) \approx 0$, т.е. явно недостаточна. Более точное приближение получается при разложении до квадратных членов, и после простых преобразований будем иметь

$$P_{\text{ЧП}} \cong \lambda_a \times \lambda_c \times t^2 / 2, \tag{15}$$

которое может быть использовано при оценке вероятностей состояний системы с отсчетом времени от момента восстановления системы после безопасного останова (аналитично (1));

б) с учетом восстановления после безопасных остановов: $T_{\text{ЗФ}}^{\text{ЧП}}$ – средние суммарные времена пребывания в состоянии до выхода в аварию $T_{\text{ЗФ}}^{\text{ЧП}} = T_c$; $T_{\text{ОФ}}^{\text{ЧП}} = T_a$; $T_{\text{ЗМТ}}^{\text{ЧП}} = T_c \times T_{\text{БО}_T} / T_b$; $T_{\text{ЗМС}}^{\text{ЧП}} = T_c \times T_{\text{БО}_C} / T_a$; $n_{\text{ЗФ}}^{\text{ЧП}}$ – среднее количество попаданий в состояния до выхода в аварию будем определять следующим образом:

$$\begin{aligned}
 n_{\text{ЗФ}}^{\text{ЧП}} &= 1 + T_c / T_b + T_c / T_a; n_{\text{ОФ}}^{\text{ЧП}} = 1 + T_c / T_a; n_{\text{ЗМС}}^{\text{ЧП}} = T_c / T_a; \\
 n_{\text{ЗМТ}}^{\text{ЧП}} &= T_c / T_b,
 \end{aligned}$$

T_a – среднее время эксплуатации системы до выхода в аварию

$$T_a = T_c + T_a + T_c \times T_{\text{БО}_T} / T_b + T_c \times T_{\text{БО}_C} / T_a.$$

Для примера рассмотрим оценку безопасности работы химического предприятия по производству жидкого базового компонента, функционирование атомного реактора подводной лодки или космического корабля.

Пусть

$$T_a = 100000; T_b = 5000; T_c = 1000000; T_{\text{БО}_T} = 1; T_{\text{БО}_C} = 48; t = 100.$$

Получим:

а) без учета восстановления после безопасных остановов

$$\begin{aligned}
 P_{\text{БФ}}(100) &= 0,9789; P_{\text{ОФ}}(100) = 10^{-4}; P_{\text{БО}_C}(100) = 10^{-3}; \\
 P_{\text{БО}_T}(100) &= 2 \times 10^{-2}; P_{\text{ЧП}}(100) \cong 5 \times 10^{-8};
 \end{aligned}$$

б) с учетом восстановления после безопасных остановов

$$\begin{aligned}
 T_{\text{ЗФ}}^{\text{ЧП}} &\approx 10^6; n_{\text{ЗФ}}^{\text{ЧП}} \approx 211; T_{\text{ОФ}}^{\text{ЧП}} \approx 10^5; n_{\text{ОФ}}^{\text{ЧП}} \approx 11; T_{\text{БО}_T} \approx 200; n_{\text{ЗМТ}}^{\text{ЧП}} \approx 200; \\
 T_{\text{БО}_C} &\approx 480; n_{\text{ЗМС}}^{\text{ЧП}} \approx 10; T_{\text{ЧП}} \approx 1100680; k_{\text{МФ}}^{\text{ЧП}} \approx 0,0909; k_{\text{ЗФ}}^{\text{ЧП}} \approx 0,909.
 \end{aligned}$$

Заметим, что $n_{\text{ОФ}}^{\text{ЧП}}$ учитывает и те попадания в состояние ОФ (нулевой длительности), которые предшествуют выходу в состояние БОС.

Величины $n_{\text{ОФ}}^{\text{ЧП}}$, $n_{\text{ЗМС}}^{\text{ЧП}}$ означают, что вероятность несрабатывания СБ на одно требование примерно равно 10^{-1} , т.е. СБ в среднем пропускает одно требование из 11. Величина $k_{\text{МФ}}^{\text{ЧП}}$ показывает, что при работе системы примерно 9 % времени она пребывает в состоянии опасного функционирования.

Если показатели $P_{\text{ОФ}}(100)$, $P_{\text{ЧП}}(100)$, $T_{\text{БФ}}$, $T_{\text{ЧП}}$ будут кажущимися оптимистическими, то показатель – коэффициент $k_{\text{МФ}}^{\text{ЧП}}$ – достаточно мал, и его величина означает осторожность в дальнейшем функционировании исследуемой системы.

Данный пример подтверждает следующие выводы.

Безопасность системы определяется надежностью СБ по отношению к опасным отказам. Имеется четыре вида ресурсных характеристик исследуемой системы:

- ресурс времени по безопасности;
- ресурс времени по безотказности;
- ресурс числа попаданий в безопасное состояние;
- ресурс числа попаданий в неработоспособное состояние.

Каждая из этих характеристик или все вместе должны использоваться в качестве критерия при оптимизации эксплуатации сложной технической системы [5].

Список литературы

1. Северцев, Н. А. Надежность сложных систем в эксплуатации и отработке / Н. А. Северцев. – М. : Высш. шк., 1989. – 431 с.
2. Дедков, В. К. Косвенные методы прогнозирования надежности / В. К. Дедков, Н. А. Северцев. – М. : ВЦ РАН, 2006. – 270 с.
3. Дивеев, А. И. Универсальные оценки безопасности / А. И. Дивеев, Н. А. Северцев. – М. : РУДН, 2005. – 86 с.
4. Северцев, Н. А. Системный анализ и моделирование безопасности / Н. А. Северцев, В. К. Дедков. – М. : Высш. шк., 2006. – 461 с.
5. Юрков, Н. К. К проблеме обеспечения безопасности сложных систем / Н. К. Юрков // Надежность и качество – 2011 : тр. междунар. симп. : в 2 т. / под ред. Н. К. Юркова. – Пенза : Изд-во ПГУ, 2011. – Т. 1. – С. 104–106.

УДК 681.31

Бецков, А. В.

Безопасность и надежность системы защиты объекта / А. В. Бецков // Надежность и качество сложных систем. – 2013. – № 1. – С. 35–40.

Бецков Александр Викторович

доктор технических наук, доцент,
Академия управления МВД России,
125171, г. Москва,
ул. Зои и Александра Космодемьянских, д. 8.
8(499) 150-10-34
E-mail: aviaspacenext@inbox.ru

Аннотация. Проводится анализ стационарных систем безопасности (СБ) объектов. Предполагается, что при ложном отказе СБ или в случае отказа объекта защиты (ОЗ) при исправной СБ система немедленно выводится в состояние безопасного останова. Отказ ОЗ при опасном отказе СБ считается недопустимым событием (авария, ЧП). Предлагается безопасность системы определять надежностью СБ по отношению к опасным отказам. Формулируются четыре вида ресурсных характеристик защищаемой системы.

Ключевые слова: объект защиты, система безопасности, отказ, авария, безопасное функционирование, случайные наработки.

A. Betskov

doctor of technical science, docent the department
Academy for control MVD of Russia
125171, Moscow,
Zoy and Alexander Kosmodemianskys street, 8.
8(499) 150-10-34
E-mail: aviaspacenext@inbox.ru

Abstract. The analysis of stationary systems of protection of objects, as the object having the safety system (SS) is carried out. It is supposed that at false refusal of SS, or in case of refusal the object of protection (OP) at serviceable SB the system is immediately removed in a condition safe останова. OP refusal at dangerous refusal of SS is considered an inadmissible event (accident, state of emergency). It is offered to determine safety of system by reliability of SS in relation to dangerous refusals. Four types of resource characteristics of protected system are formulated

Key words: object of protection, safety system, refusal, accident, safe functioning, casual practices.