ФУНДАМЕНТАЛЬНЫЕ ОСНОВЫ БЕЗОПАСНОСТИ, НАДЕЖНОСТИ И КАЧЕСТВА

УДК 629.039.58

ПОЛУМАРКОВСКАЯ МОДЕЛЬ ИССЛЕДОВАНИЯ БЕЗОПАСНОСТИ СИСТЕМ. БЕЗОПАСНОСТЬ И НАДЕЖНОСТЬ СИСТЕМЫ КАК ОБЪЕКТА, ИМЕЮЩЕГО СИСТЕМУ ЗАЩИТЫ

Н. А. Северцев, А. В. Бецков, Ю. В. Лончаков

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);
– $БО_с$ – безопасный останов вследствие отказа ОЗ при работоспособном СБ (предотвращение ЧП);
– $БО_т$ – 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).

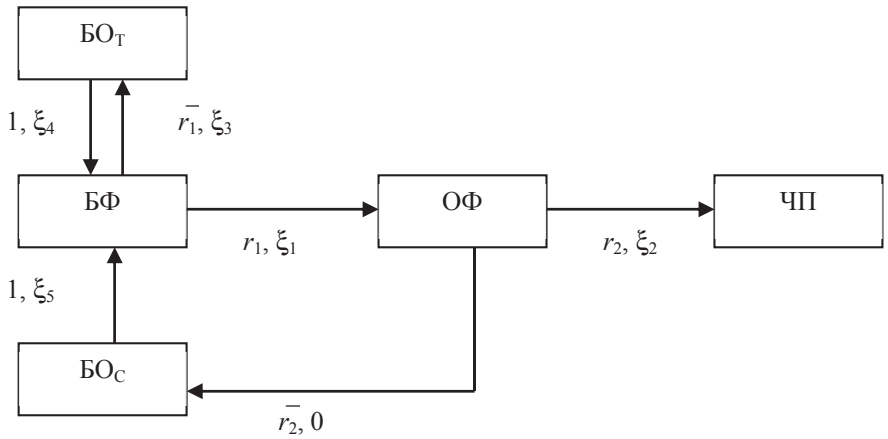

Рис. 1. Граф состояний и переходов функционирования системы:
r_i – вероятность перехода, $\bar{r}_i = 1 - r_i$; ξ – случайное время до перехода в i-состояние

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 $b \le c$ 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).

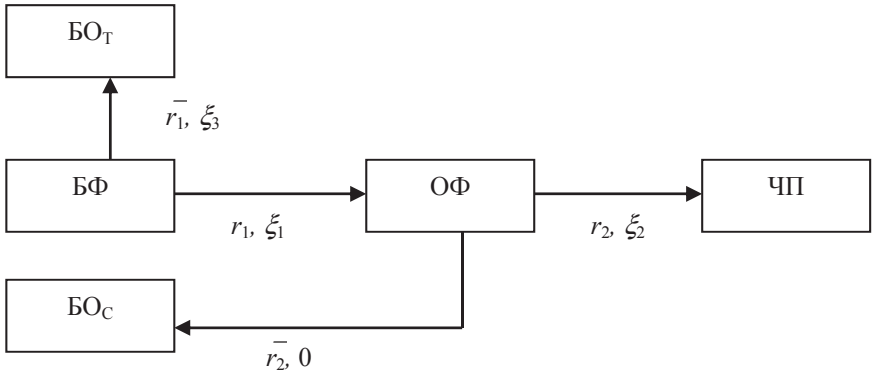

Рис. 2. Граф состояний и переходов полумарковской модели

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

Состояние системы в некоторый момент t будем описывать многозначной логической (индикаторной) переменной $Q \in \Omega = \{БО_Т, БО_С, ОФ, ЧП\}$. 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, которое, в свою очередь, соответствует некоторому состоянию системы – $Q(\upsilon)$ 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.

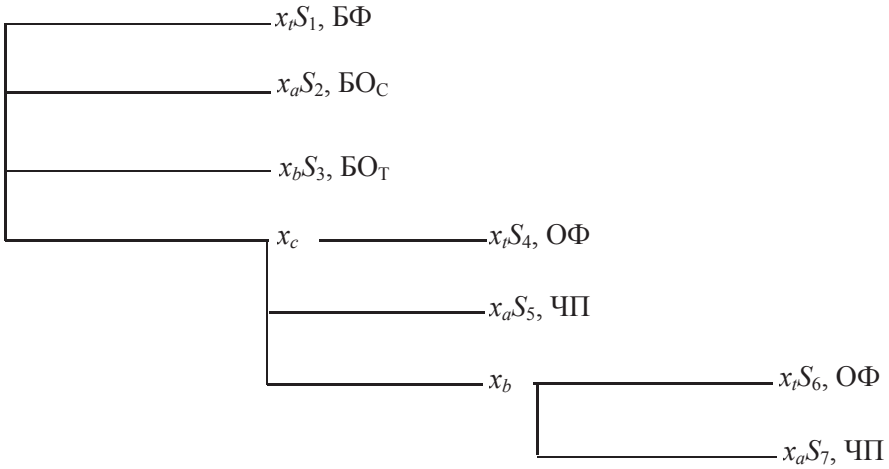

Рис. 3. Усеченное последовательное дерево событий ОЗ – СБ

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

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

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

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

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

Тогда

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

$$P_3 = \int_0^t \overline{F}_a(x) \times \overline{F}_c(x) d_a(t); P_4 = F_c(t) \times \overline{F}_a(t) \times F_b(t); P_5 = \int_0^t F_c(x) \times \overline{F}_b(x) dF_a(x);$$

$$P_6 = \overline{F}_a(t) \times \int_0^t F_c(x) dF_b(x); P_7 = \int_0^t \int_0^x F_c(y) dF_b(y) dF_a(y). \quad (1)$$

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:

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

$$P_{БО_С}(t) = P\{Q(t) = БО_С\} = P_2(t);$$

$$P_{БО_Т}(t) = P\{Q(t) = БО_Т\} = P_3(t);$$

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

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

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

$$P_{БО_Т}(\infty) = \overline{r}_1 = 1 - r_i; P_{БО_Т}(\infty) = r_1 \times \overline{r}_2 = r_1 \times (1 - r_2);$$

$$P_{ЧП}(\infty) = r_2 \times r_1.$$

Откуда

$$r_1 = 1 - P_{БО_Т}(\infty), r_2 = 1 - P_{БО_С}(\infty) / r_1. \quad (3)$$

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

$$F_{\xi_1}(t) = P_{БО_Т}(t) / P_{БО_Т}(\infty); F_{\xi_1}(t) = P_{БО_С}(t) / P_{БО_С}(\infty). \quad (4)$$

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

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

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

Здесь $\overline{F}(t) = 1 - F(t)$.

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):

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

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

$$T_{\text{ЧП}} = T_{\text{БФ}} / (r_1, r_2) + T_{\text{ОФ}} / r_2 + \overline{r}_1 T_{\text{БО}_\text{Т}} / (r_1, r_2) + \overline{r}_2 T_{\text{БО}_\text{С}} / r_2. \tag{7}$$

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

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

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

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

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

$$T_{\text{ЗМТ}}^{\text{ЧП}} = \overline{r}_2 T_{\text{ЗМС}}^{\text{ЧП}} / r_2;\ n_{\text{ЗМС}}^{\text{ЧП}} = \overline{r}_2 / r_2. \tag{10}$$

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

$$k_{\text{МФ}}^{\text{ЧП}} = T_{\text{ОФ}}^{\text{ЧП}} \Big/ \left(T_{\text{ЗФ}}^{\text{ЧП}} + T_{\text{ОФ}}^{\text{ЧП}}\right). \tag{11}$$

Данный коэффициент показывает, насколько опасна работающая исследуемая система.

2. Коэффициент безопасности функционирования системы

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

Рассмотрим задачу для случая, когда наработки a, b, c имеют экспоненциальное распределение с параметрами λ_a, λ_b, λ_c. Соответственно обозначим:

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

Запишем следующие соотношения:

а) без учета восстановлений после безопасных остановов:

$$P_{\text{БФ}} = \exp(-\lambda^* \times t);\ P_{\text{БО}_\text{С}} = P_{\text{БФ}} \times \lambda_a / \lambda^*;$$

$$P_{\text{БО}_\text{т}} = P_{\text{БФ}} \times \lambda_b / \lambda^*;$$

$$P_{\text{ОФ}} = \exp(-\lambda_0 \times t) \times (1 - \exp(-(\lambda_b + \lambda_c) \times t) \times \lambda_c / (\lambda_b + \lambda_c);$$

$$P_{\text{ЧП}} = (1 - \exp(-\lambda_a \times t)) \times \lambda_c / (\lambda_b + \lambda_c) - (1 - \exp(-\lambda^* \times t) \times \lambda_a \lambda_c / \lambda^* (\lambda_b + \lambda_c);$$

$$P_{\text{БО}_C}(\infty) = \lambda_a / \lambda^*;\ P_{\text{БО}_T}(\infty) = \lambda_b / \lambda^*;\ P_{\text{ЧП}}(\infty) = \lambda_c / \lambda^*;$$

$$r_1 = (\lambda_a + \lambda_c) / \lambda^*;\ r_2 = \lambda_c / (\lambda_a + \lambda_c);$$

$$M\xi_1 = T^*;\ M\xi_2 = T_a;\ M\xi_3 = T^*. \qquad (13)$$

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

$$P_{\text{БФ}} \cong 1 - \lambda^* \times t;\ P_{\text{БО}_\text{С}} \approx \lambda_a \times t;\ P_{\text{БО}_\text{т}} \approx \lambda_b \times t, \qquad (14)$$

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 не достаточна. Более точное приближение получается при разложении до квадратных членов, и после простых преобразований будем иметь

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

которое может быть использовано при оценке вероятностей состояний системы с отсчетом времени от момента восстановления системы после безопасного останова (аналогично (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:

$$n_{\text{ЗФ}}^{\text{ЧП}} = 1 + T_\text{с} / T_b + T_c / T_a;\ n_{\text{ОФ}}^{\text{ЧП}} = 1 + T_c / T_a;\ n_{\text{ЗМС}}^{\text{ЧП}} = T_c / T_a;$$

$$n_{\text{ЗМТ}}^{\text{ЧП}} = T_c / T_b;$$

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, функционирования атомного реактора подводной лодки или космического корабля.

Пусть

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

Получим:

а) без учета восстановления после безопасных остановов

$$P_{\text{БФ}}(100) = 0{,}9789;\ P_{\text{ОФ}}(100) = 10^{-4};\ P_{БО_\text{С}}(100) = 10^{-3};$$

$$P_{\text{БО}_\text{т}}(100) = 2 \times 10^{-2};\ P_{\text{ЧП}}(100) \cong 5 \times 10^{-8};$$

б) с учетом восстановления после безопасных остановов

$$T_{\text{ЗФ}}^{\text{ЧП}} \approx 10^6;\ n_{ЗФ}^{ЧП} \approx 211;\ T_{\text{ОФ}}^{\text{ЧП}} \approx 10^5;\ n_{\text{ОФ}}^{\text{ЧП}} \approx 11;\ T_{\text{БО}_\text{т}} \approx 200;\ n_{\text{ЗМТ}}^{\text{ЧП}} \approx 200;$$

$$T_{\text{БО}_C} \approx 480;\ n_{\text{ЗМС}}^{\text{ЧП}} \approx 10;\ T_{\text{ЧП}} \approx 1100680;\ k_{\text{МФ}}^{\text{ЧП}} \approx 0{,}0909;\ k_{\text{ЗФ}}^{\text{ЧП}} \approx 0{,}909.$$

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

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

Если показатели $P_{ОФ}(100)$, $P_{ЧП}(100)$, $T_{БФ}$, $T_{ЧП}$ будут кажущими оптимистическими, и при этом коэффициент $k_{МФ}^{ЧП}$ достаточно мал, следует проявить особую осторожность в дальнейшем функционировании исследуемой системы.

Данный пример подтверждает следующие выводы.

Безопасность системы определяется надежностью СБ по отношению к опасным отказам [4–7]. Имеются 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.

Список литературы

1. Северцев, Н. А. Надежность сложных систем в эксплуатации и отработке / Н. А. Северцев. – М. : Высшая школа, 1989. – 431 с.
2. Северцев, Н. А. Косвенные методы прогнозирования надежности / Н. А. Северцев, В. К. Дедков. – 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 теории безопасности / Н. А. Северцев, А. В. Бецков. – М. : МГУ им. М. В. Ломоносова, 2009. – 452 с.
5. Затылкин, А. В. Алгоритмическое и программное обеспечение расчета параметров статически неопределимых систем амортизации РЭС / А. В. Затылкин, Г. В. Таньков, И. И. Кочегаров // Надежность и качество сложных систем. – 2013. – № 4. – С. 33–40.
6. Юрков, Н. К. К проблеме обеспечения глобальной безопасности / Н. К. Юрков // Надежность и качество : тр. Междунар. симп. : в 2 т. / под ред. Н. К. Юркова. – Пенза : Изд-во ПГУ, 2012. – Т. 1. – С. 6–7.
7. Батаева, И. П. Защита информации и информационная безопасность / И. П. Батаева // Надежность и качество : тр. Междунар. симп. : в 2 т. / под ред. Н. К. Юркова. – Пенза : Изд-во ПГУ, 2012. – Т. 1. – С. 116–118.

УДК 629.039.58

Северцев, Н. А.

Полумарковская модель исследования безопасности систем. Безопасность и надежность системы как объекта, имеющего систему защиты / Н. А. Северцев, А. В. Бецков, Ю. В. Лончаков // Надежность и качество сложных систем. – 2014. – № 1(5). – С. 2–8.

Северцев Николай Алексеевич
доктор технических наук, профессор,
заслуженный деятель науки и техники
Российской Федерации, лауреат премий
Правительства Российской Федерации
и Совета Министров СССР, лауреат международной
Золотой медали Леонардо Да Винчи
в области изобретательства,
заведующий отделом ВЦ РАН
им. А. А. Дородницына.
(119333, Россия, г. Москва ул. Вавилова, 40)
(495) 135-55-08
E-mail: severcev@mail.ru

Severtsev Nikolay Alekseevich
doctor of technical scienses, professor,
the honored worker of science and equipment
of the Russian Federation, the winner of awards
of the Government of the Russian Federation
and Council of ministers of the USSR,
the winner of the international Gold medal
Leonardo Da Vinci in the field of invention,
the head of department
of VTs Russian Academy of Sciences
of A. A. Dorodnitsyn.
(119333, 40 Vavilov street, Moscow, Russia)

Бецков Александр Викторович
доктор технических наук, доцент,
Академия управления МВД России,
(125171, Россия, г. Москва,
ул. З. и А. Космодемьянских, 8)
(499) 745-95-20
E-mail: abckov@mail.ru
Лончаков Юрий Валентинович
доктор технических наук, летчик-космонавт,
Герой России,
помощник руководителя ФКА Роскосмос
(107996, ГСП-6, г. Москва, ул. Щепкина, 42)
(495) 688-90-60
E-mail: lonchakov@mail.ru

Аннотация. Предложен результат исследования безопасности и надежности особо важной стационарной системы, имеющей собственную защиту, на основе полумарковской модели. За основу взяты три «базовых» состояния собственной системы безопасности: работоспособном, ложного отказа, истинного отказа (опасного отказа).

Ключевые слова: полумарковская модель, безопасность, надежность, система защиты, объект защиты, система безопасности, чрезвычайное происшествие, безопасное функционирование, опасное функционирование, коэффициент безопасности функционирования системы.

Betskov Aleksandr Viktorovich
doctor of technical scienses, associate professor,
Academy of management of the Ministry
of Internal Affairs of Russia,
(125171, 8 Z. and A. Kosmodemjanskih street,
Moscow, Russia)

Lonchakov Yuriy Valentinovich
doctor of technical scienses, the space pilot,
Hero of Russia, the assistant administrator
of FKA Roskosmos
(107996, GSP-6, 42 Shchepkin street, Moscow, Russia)

Abstract. In work the result of research of a security and on especially important stationary systems having own protection, on the basis of polumarkovsk is offered to model. For a basis three «base» conditions of system of a security are taken: efficient, false refusal, true refusal (dangerous refusal).

Key words: polumarkovska model, a security, reliability, system of protection, object of protection, system of a security, emergency, without functioning, dangerous functioning, factor of a security of functioning of system.