

## МОДЕЛЬ ЭЛЕМЕНТА СИСТЕМЫ ЗАЩИТЫ КРИТИЧЕСКИ ВАЖНОГО ОБЪЕКТА

С целью обеспечения безопасности информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность функционирующих в составе критически важных объектов (КВО) Российской Федерации информационных систем и телекоммуникационных сетей, деструктивные информационные воздействия на которые могут привести к значительным негативным последствиям, проводятся исследования защиты функционирования КВО в соответствии с [1].

В настоящее время разработаны модели, позволяющие исследовать функционирование отдельных систем защиты (СЗ) КВО при воздействии некоторых возмущающих факторов. Однако при оценке уровня защищенности КВО, обеспечиваемого перспективной СЗ, необходимо учитывать множество разнородных случайных возмущающих факторов (ВФ). Модели, описывающей с единых позиций функционирование СЗ КВО с учетом совокупности разнородных случайных возмущающих факторов, не разработано.

Поэтому задача оценки уровня защищенности КВО, обеспечиваемого элементом СЗ с учетом действия всей совокупности возмущающих факторов, является актуальной, имеет важное теоретическое и практическое значение, и для ее решения требуется совершенствование формальных методов анализа элементов и систем КВО.

Для исследования основных процессов, протекающих в элементах защиты КВО на основе имитации свойств технических средств и внешних воздействий, необходимо математически описать свойства элементов СЗ КВО и внешних воздействий, т. е. построить математические модели, описывающие эволюцию состояний элемента СЗ КВО и появление внешних воздействий. В статье рассмотрена постановка и приведено решение задачи определения характеристик потока воздействий ВФ, прошедших через элемент СЗ КВО.

Общее описание процессов, рассматриваемых в настоящей работе, состоит в следующем.

Нахождение элемента СЗ КВО в том или ином состоянии (эволюция элемента) описывается некоторым случайным процессом  $\xi(t)$  с фазовым пространством  $E$ . Будем считать, что множество  $E$  состоит из непересекающихся подмножеств: подмножества состояний отказа  $E_0$  и состояний работоспособности  $E_1$ :  $E = E_0 \cup E_1$ ,  $E_0 \cap E_1 = \emptyset$ . Множество состояний  $E_1$  считаем работоспособным, и если воздействие поступает в момент, когда элемент системы защиты находится в состоянии  $i \in E_1$ , то воздействие не проходит, множество  $E_0$  включает в себя состояния неработоспособности, и если воздействие поступает в момент, когда элемент системы защиты находится в состоянии  $i \in E_0$ , то имеет место «нежелательное событие», приводящее к преодолению защиты, обеспечиваемой элементом СЗ КВО.

Предполагается, что моменты появления возмущающих воздействий образуют некоторый процесс однородных событий.

Необходимо исследовать поток событий, которые происходят в моменты времени появления возмущающих воздействий, попавших в систему тогда, когда элемент системы находился в состоянии  $E_0$  — состоянии неработоспособности. Предполагается, что когда элемент СЗ КВО работоспособен в момент поступления возмущающего воздействия, то это воздействие теряется, а в противном случае возмущающее воздействие проходит элемент СЗ КВО, образуя нежелательное событие. Под возмущающим воздействием (возмущающим фактором) в данном случае понимаются помехи, сбои, отказы и результаты целенаправленных действий нарушителя.

Будем предполагать, что эволюция состояний элемента СЗ КВО описывается полумарковским процессом  $\xi(t)$  с конечным множеством состояний  $E$  и полумарковской матрицей  $Q_{ij}(t)$ ,  $i, j \in E$ ,  $t \in R^+$ .

Относительно моментов появления возмущающих факторов будем полагать, что они образуют пуассоновский поток с параметром  $\lambda$ . Такое предположение делается в силу того, что процесс возмущающих воздействий можно представить в виде суммы большого числа независимых редких потоков воздействий, образующих в конечном итоге поток возмущающих факторов. В таком случае суммарный предельный поток возмущающих факторов на основании предельной теоремы Григелиониса является пуассоновским потоком [2, 3].

Ставится задача определения функции распределения момента первого появления «нежелательного события» — момента первого пропуска внешнего воздействия.

Описанные выше процессы укладываются в общую модель полумарковского процесса с «катастрофами» [3]. Подобные задачи рассматривались А. Д. Соловьевым [4] для регенерирующих процессов.

Если полумарковский процесс  $\xi(t)$ , описывающий эволюцию элемента СЗ КВО, является управляемым, то можно ставить оптимизационную задачу, например задачу выбора оптимального управления, максимизирующего математическое ожидание времени до первого пропуска внешнего воздействия [4], преодолевшего защиты.

Определим общие соотношения, позволяющие разработать алгоритм вычисления искомых характеристик внешнего воздействия, прошедшего через элемент СЗ КВО, и покажем возможности описанной модели на частном примере — марковский случай с двумя состояниями, в котором решение поставленной задачи получается в замкнутом виде. Для этого частного случая можно получить характеристики потока моментов воздействия всей совокупности внешних возмущающих факторов (функцию распределения времени результирующего воздействия, прошедшего элемент СЗ КВО).

Так как для марковского случая момент первого пропуска внешнего воздействия происходит в моменты реализации марковски зависимых событий, то, очевидно, поток моментов пропуска воздействия возмущающих факторов образует процесс восстановлений с запаздыванием. Его вероятностные характеристики будут получены ниже.

Решение задачи определения функции распределения времени между моментами прохода воздействий потока возмущающего фактора на выходе элемента СЗ КВО проводится в следующей последовательности.

### 1. Описание состояний элемента системы защиты КВО

Эволюция состояний элемента СЗ КВО описывается тремя основными характеристиками: полумарковским процессом с конечным множеством состояний; полумарковской матрицей и начальным распределением вероятностей состояний полумарковского процесса  $p_i = P(\xi(0) = i)$ ,  $i \in E$ .

Смена состояний полумарковского процесса  $\xi(t)$ ,  $p_{ij} \geq 0$ ;  $\sum p_{ij} = 1$ ,  $j \in E$ , описывается матрицей переходных вероятностей вложенной цепи Маркова вида  $p_{ij} = Q_{ij}(\infty) = \lim_{t \rightarrow \infty} Q_{ij}(t)$ . При этом  $P(0 < t / \xi(0) = i) = \sum Q_{ij}(t)$ ,  $j \in E$ , есть условное распределение времени непрерывного пребывания процесса  $\xi(t)$  в фиксированном состоянии при условии, что это состояние  $i \in E$ .

Обозначим через  $\tau$  случайное время до первого пропуска внешнего воздействия, соответствующие условные распределения времени непрерывного пребывания процесса  $\xi(t)$  в фиксированном состоянии при начальном условии  $\xi(0) = i$  обозначим в виде соотношений  $\Phi_i(t) = P(\tau < t / \xi(0) = i)$ ,  $\bar{\Phi}_i(t) = P(\tau \geq t / \xi(0) = i)$ .



Тогда по формуле полной вероятности, учитывая, что смена состояний полумарковского процесса осуществляется в марковские моменты времени, имеем:

$$\begin{cases} \bar{\Phi}_i(t) = 1 - \sum_{j \in E} Q_{ij}(t) + \sum_{j \in E} \int_0^t \bar{\Phi}_j(t-x) dQ_{ij}(x), & i \in E_1; \\ \bar{\Phi}_i(t) = e^{-\lambda \cdot t} (1 - \sum_{j \in E} Q_{ij}(t)) + \sum_{j \in E} \int_0^t \bar{\Phi}_j(t-x) e^{-\lambda \cdot x} dQ_{ij}(x), & i \in E_0; \\ \bar{\Phi}(t) = P(\tau \geq t) = \sum_{i \in E} P(\tau \geq t / \xi(0) = i) = \sum_{i \in E} p_i \bar{\Phi}_i(t). \end{cases} \quad (1)$$

Систему интегральных уравнений (1) можно решить методом Лапласа, так как в нее входят интегралы свертки. В этом случае основная трудность заключается в обращении преобразования Лапласа для получения решения.

Ситуация значительно упрощается, если необходимо исследовать математическое ожидание времени до первого пропуска внешнего воздействия, прошедшего элемент СЗ КВО.

Обозначим математическое ожидание времени до первого пропуска внешнего воздействия  $M_i = M(\tau / \xi(0) = i)$ . Тогда по формуле полного математического ожидания имеем:

$$\begin{cases} M_i = \int_0^\infty (1 - \sum_{j \in E} Q_{ij}(t)) dt + \sum_{j \in E} p_{ij} M_j, & i \in E_1, \\ M_i = \int_0^\infty (1 - \sum_{j \in E} Q_{ij}(t)) \cdot e^{-\lambda \cdot t} dt + \sum_{j \in E} M_j \int_0^\infty e^{-\lambda \cdot x} dQ_{ij}, & i \in E_0 \\ M = M(\tau) = \sum_{i \in E} p_i \cdot M_i. \end{cases} \quad (2)$$

Система линейных алгебраических уравнений (2) решается аналитически, и ответ получается в замкнутом виде.

## 2. Описание состояний элемента СЗ КВО с учетом процесса восстановления

Пусть эволюция состояний элемента СЗ КВО описывается альтернирующим процессом восстановления с распределениями  $F_0(t)$  и  $F_1(t)$ . Значит, полумарковский процесс  $\xi(t)$  имеет два состояния  $E_0 = \{0\}$ ;  $E_1 = \{1\}$  и полумарковская матрица имеет вид:  $Q_{01}(t) = F_0(t)$ ;  $Q_{10}(t) = F_1(t)$ ;  $Q_{00}(t) = Q_{11}(t) = 0$ . Подставляя эти характеристики в систему (1), получаем:

$$\begin{cases} \bar{\Phi}_1(t) = \bar{F}_1(t) + \int_0^t \bar{\Phi}_0(t-x) dF_1(x); \\ \bar{\Phi}_0(t) = e^{-\lambda \cdot t} \bar{F}_0(t) + \int_0^t \bar{\Phi}_1(t-x) e^{-\lambda \cdot x} dF_0(x); \\ \bar{\Phi}(t) = P(\tau \geq t) = \sum_{i=0}^1 p_i \bar{\Phi}_i(t), \end{cases} \quad (3)$$

где обозначено  $\bar{F}_i(t) = 1 - F_i(t)$ ;  $i = 0, 1$ .

Далее обозначим через  $A^*(p)$  для произвольной функции  $A(x)$ ,  $x \geq 0$ , ее преобразование Лапласа:

$$A^*(p) = \int_0^\infty e^{-pt} A(x) dx.$$

Тогда из системы уравнений (3) имеем:

$$\begin{cases} \bar{\Phi}_1^*(p) = \bar{F}_1^*(p) + (1 - p \bar{F}_1^*(p)) \bar{\Phi}_0^*(p); \\ \bar{\Phi}_0^*(p) = \bar{F}_0^*(p + \lambda) + (1 - (p + \lambda) \bar{F}_0^*(p + \lambda)) \bar{\Phi}_1^*(p). \end{cases} \quad (4)$$



Откуда находим:

$$\begin{cases} \overline{\Phi}_1^*(p) = \frac{\overline{F}_1^*(p) + \overline{F}_0^*(p + \lambda)(1 - p\overline{F}_1(p))}{1 - (1 - p\overline{F}_1^*(p))(1 - (p + \lambda)\overline{F}_0^*(p + \lambda))}; \\ \overline{\Phi}_0^*(p) = \frac{\overline{F}_0^*(p + \lambda) + \overline{F}_1^*(p)(1 - (p + \lambda)\overline{F}_0^*(p + \lambda))}{1 - (1 - p\overline{F}_1^*(p))(1 - (p + \lambda)\overline{F}_0^*(p + \lambda))}. \end{cases} \quad (5)$$

Так как  $M_i = \overline{\Phi}_i^*(0)$  получаем из (5) решение в виде:

$$\begin{cases} M_1 = \frac{\int_0^\infty \overline{F}_1^*(x) dx + \int_0^\infty e^{-\lambda x} \overline{F}_0(x) dx}{\lambda \cdot \int_0^\infty e^{-\lambda x} \overline{F}_0(x) dx}; \\ M_0 = -\int_0^\infty \overline{F}_1(x) dx + \frac{\int_0^\infty \overline{F}_1(x) dx + \int_0^\infty e^{-\lambda x} \overline{F}_0(x) dx}{\lambda \cdot \int_0^\infty e^{-\lambda x} \overline{F}_0(x) dx}. \end{cases} \quad (6)$$

Таким образом, полученное решение в явном виде характеризует математическое ожидание времени до первого пропуска внешнего воздействия, прошедшего элемент СЗ КВО.

### 3. Случай экспоненциального распределения процессов восстановления и отказов

Теперь упростим задачу, положив для альтернирующего процесса функцию распределения процесса восстановления и процесса отказа в экспоненциальном виде:  $\overline{F}_0(t) = e^{-\mu t}$ ,  $\overline{F}_1(t) = e^{-\lambda_p t}$ ,  $t \geq 0$ .

Тогда преобразование Лапласа функций распределения процесса восстановления и процесса отказа в данном случае будет иметь вид:

$$\overline{F}_0(p) = \frac{1}{p + \mu}; \quad \overline{F}_1(p) = \frac{1}{p + \lambda_p}.$$

Подставляя эти функции в равенства (5), имеем:

$$\begin{cases} \overline{\Phi}_1^*(p) = \frac{p + \lambda + \mu + \lambda_p}{p^2 + p(\lambda + \mu + \lambda_p)^2 + \lambda_p \lambda}; \\ \overline{\Phi}_0^*(p) = \frac{p + \mu + \lambda_p}{p^2 + p(\lambda + \mu + \lambda_p)^2 + \lambda_p \lambda}. \end{cases} \quad (7)$$

Решение системы (7) для изображений получается в следующем виде:

$$M_1 = \frac{\lambda + \mu + \lambda_p}{\lambda_p \cdot \lambda}; \quad M_0 = \frac{\mu + \lambda_p}{\lambda_p \cdot \lambda}. \quad (8)$$

Обращение преобразования Лапласа системы (7) дает:

$$\begin{cases} \overline{\Phi}_0(t) = \frac{a_2 - \lambda}{a_2 - a_1} \cdot e^{a_1 t} + \frac{a_1 - \lambda}{a_1 - a_2} \cdot e^{a_2 t}; \\ \overline{\Phi}_1(t) = \frac{a_2}{a_2 - a_1} \cdot e^{a_1 t} + \frac{a_1}{a_1 - a_2} \cdot e^{a_2 t}, \end{cases} \quad (9)$$

$$\text{где } a_{1,2} = -\frac{\lambda + \mu + \lambda_p}{2} \pm \sqrt{\frac{1}{4}(\lambda + \mu + \lambda_p)^2 - \lambda_p \lambda}.$$

Легко убедиться, что корни  $a_i$  знаменателя в (7) различные, действительные и отрицательные, поэтому и справедливы равенства (9).

На практике представляет интерес вид функции распределения момента времени первого пропуска внешнего воздействия в стационарном случае.

Тогда  $P_0 = \frac{\lambda_p}{\lambda_p + \mu}$ ;  $P_1 = \frac{\mu}{\lambda_p + \mu}$ , а соответствующие распределения и математические ожидания вычисляются по формулам:

$$\overline{\Phi}(t) = \sum_{i=0}^1 p_i \cdot \overline{\Phi}_i(t); \quad M = \sum_{i=0}^1 p_i \cdot M_i. \quad (10)$$



Заметим, что для марковского случая, рассматриваемого в настоящем исследовании, аналогичный результат можно получить другим методом, если построить новый марковский процесс с поглощающим состоянием, в которое переходит марковский процесс в момент первого пропуска возмущающего фактора, а затем выписать и решить систему дифференциальных уравнений Колмогорова для вероятностей состояний этого процесса в произвольный момент времени  $t$ .

В силу того, что моменты пропуска возмущающих факторов являются марковскими, поток этих моментов является потоком восстановления с запаздыванием, у которого распределение первого интервала определяется равенством  $\Psi_1(t) = 1 - \bar{\Phi}(t)$  в зависимости от начального распределения  $(P_0, P_1)$ , а распределение последующих интервалов определяется равенством  $\Psi(t) = 1 - \bar{\Phi}_0(t)$ , так как в этом случае начальные условия имеют вид  $P_0 = 1, P_1 = 0$ .

Определим функцию распределения времени между моментами смежных воздействий потока возмущающих факторов, прошедших через элемент системы защиты КВО. Для этого введем в рассмотрение случайную величину  $\xi(t)$ , принимающую три возможных значения:

$$\xi(t) = \begin{cases} 1, & \text{поток ВФ проходит через элемент СЗ КВО;} \\ 2, & \text{поток ВФ не проходит через элемент СЗ КВО;} \\ 3, & \text{поглощающее состояние.} \end{cases}$$

Поглощающее состояние означает появление события, заключающегося в том, что через элемент СЗ КВО прошло смежное (следующее после предыдущего) воздействие потока ВФ. Требуется составить те уравнения, которым удовлетворяют вероятности  $P_j(t) = P(\xi(t) = j / \xi(0) = 1), j = 1, 2, 3$ .

Для определения вероятностей  $P_j(t)$  составляется система уравнений и задаются начальные условия. С этой целью рассмотрим стационарное распределение альтернирующего процесса, который имеет место в данном случае.

Альтернирующий процесс характеризуется двумя параметрами:

$\lambda_p$  — интенсивностью отказов элемента СЗ КВО;

$\mu$  — интенсивностью восстановления элемента СЗ КВО.

Стационарное (равномерное) распределение альтернирующего процесса описывается интенсивностями реализации событий:

$$\pi_1 = \frac{1/\lambda_p}{(1/\mu + 1/\lambda_p)}; \quad \pi_2 = \frac{1/\mu}{1/\mu + 1/\lambda_p}, \quad (11)$$

где  $\pi_1$  — стационарная интенсивность работы элемента СЗ КВО;

$\pi_2$  — стационарная интенсивность восстановления элемента СЗ КВО.

Следовательно, начальные условия для системы уравнений имеют вид:

$$t = 0: \quad P_1(0) = p_1, \quad P_2(0) = p_2, \quad P_3(0) = 0. \quad (12)$$

Интегрирование системы дифференциальных уравнений с начальными условиями (12) дает искомую функцию распределения времени между моментами прохода смежных воздействий потока ВФ на выходе элемента СЗ КВО. Эта система уравнений Колмогорова с использованием метода преобразования Лапласа сводится к системе алгебраических уравнений. Применяя метод Гаусса к этой системе, получим решение для изображения (преобразования Лапласа) оригинала функции распределения. Используя обратное преобразование Лапласа, определим соотношение для оригинала функции распределения времени между моментами прохода воздействий потока возмущающего фактора на выходе первого элемента СЗ КВО:

$$P_3(t) = 1 - \frac{\lambda \lambda_p (e^{-a_1 t} - e^{-a_2 t})}{(\mu + \lambda_p) \sqrt{(\mu + \lambda_p + \lambda)^2 - 4\lambda_p \lambda}}, \quad (13)$$

$$\text{где } a_{1,2} = -\frac{\lambda + \mu + \lambda_p}{2} \pm \sqrt{\frac{1}{4}(\lambda + \mu + \lambda_p)^2 - \lambda_p \lambda}.$$

Графики функции  $P_3(t)$  в зависимости от  $\lambda$ ,  $\lambda_p$  и  $\mu$  представлены на рис. 1–3. Использование соотношения (13) и графических зависимостей функции распределения времени между моментами прохода воздействий потока возмущающего фактора на выходе элемента СЗ КВО (рис. 1–3) позволяет по известным характеристикам случайных ВФ на входе элемента СЗ КВО и заданным параметрам элемента СЗ КВО определить характеристики ВФ, прошедших через элемент СЗ КВО, а также дает возможность назначать оптимальное время проведения плановых предупредительных профилактик элементов СЗ КВО.

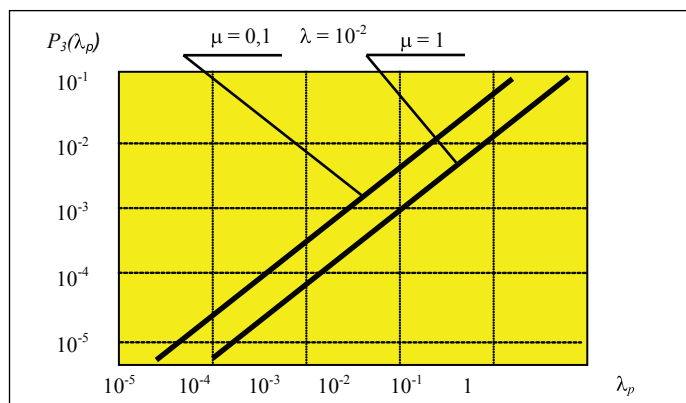


Рис. 1. График функции  $P_3(t)$  в зависимости от параметра  $\lambda_p$

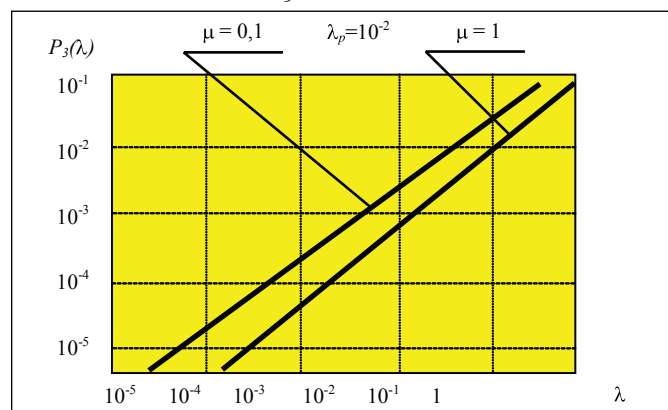


Рис. 2. График функции  $P_3(t)$  в зависимости от параметра  $\lambda$

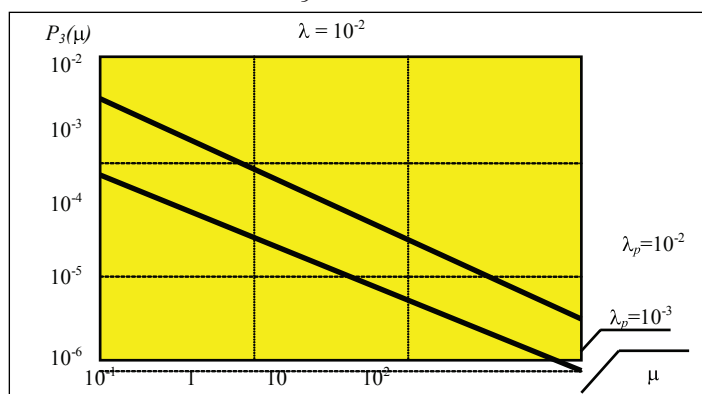


Рис. 3. Графики функции  $P_3(t)$  в зависимости от параметра  $\mu$

Таким образом, разработана стохастическая модель элемента системы защиты для исследования основных процессов, протекающих в элементах СЗ КВО, при имитации свойств технических средств защиты и внешних воздействий. Математически описаны свойства

элементов СЗ КВО и внешних воздействий. Рассмотрена постановка и приведено решение задачи определения характеристик потока воздействий возмущающих факторов, прошедших через элемент СЗ КВО.

Использование разработанной модели позволяет анализировать процесс функционирования сложных по своей структуре систем защиты КВО. Система защиты может быть представлена в виде последовательно-параллельного соединения элементов СЗ КВО. Исходные данные для применения модели задаются соответствующими интенсивностями потоков воздействий возмущающих факторов (помех, сбоев, отказов и результатов целенаправленных действий нарушителя) и внутренними параметрами элементов СЗ КВО (интенсивностями отказов и восстановлений), которые могут быть получены путем анализа эксплуатационной и технической документации КВО. Практическая ценность предлагаемой модели заключается в возможности оценивать уровни защищенности, обеспечиваемые СЗ КВО, при действии совокупности разнородных возмущающих факторов.

## СПИСОК ЛИТЕРАТУРЫ:

1. Указ Президента РФ от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» (с изменениями от 22 марта, 20 июля 2005 г., 30 ноября 2006 г., 23 октября, 17 ноября 2008 г.).
2. Математическая энциклопедия. Т. 4. М.: Советская энциклопедия, 1984.
3. Каштанов В. А., Янышевский И. М. Теория вероятностей и ее применение. Выпуск IV. 1996.
4. Вопросы математической теории надежности / Под ред. Б. В. Гнеденко. М.: Радио и связь, 1984.