С.В. Скрыль,
доктор технических наук, профессор

А.А. Окрачков,
кандидат технических наук,
Военный учебно-научный центр (Воронеж)

МЕТОД КОЛИЧЕСТВЕННОЙ ОЦЕНКИ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

METHOD OF QUANTITATIVE ESTIMATION OF EFFICIENCY INDICATORS OF INFORMATION PROTECTION SYSTEMS AGAINST UNAUTHORIZED ACCESS

Разработан метод количественной оценки показателей эффективности систем защиты информации от несанкционированного доступа. Метод основан на представлении динамики функционирования СЗИ НСД конечным полумарковским процессом, характеризующимся полумарковской матрицей.

Method of quantitative estimation of efficiency indicators of information security systems is developed. The method is based on the representation of the dynamics of the operation of systems to protect information from unauthorized access to end the semi-Markov process, characterized by a semi-Markov matrix.

Модели исследования математических свойств динамики функционирования СЗИ НСД для комплексной оценки их эффективности представляют собой математические модели комплексной оценки показателей эффективности СЗИ НСД , отражающих данные математические свойства [1]. Комплексная оценка эффективности СЗИ НСД осуществляется с помощью интегрального показателя, оцениваемого через элементарные показатели эффективности СЗИ НСД. Элементарные показатели эффективности СЗИ НСД как объекты контроля можно разделить на качественные ($Е_ф$, $Е_{уи}$) и количественный ($Е_{кф}$). Обозначим элементарные показатели СЗИ НСД как объекты контроля следующим образом: $Е_ф$ — показатель функциональности СЗИ НСД; $Е_{кф}$ — показатель корректности функционирования СЗИ НСД; $Е_{уи}$ — показатель удобства использования СЗИ НСД.

Оценку показателей $Е_ф$, $Е_{уи}$ целесообразно осуществлять на основе анализа программной документации на СЗИ НСД при помощи качественной шкалы, предполагающей лингвистическую оценку в виде одного из значений «допустимо», «недопустимо», что дает возможность введения булевой переменной. При этом значение, равное 1, интерпретируется как допустимая эффективность функционирования, а 0 — недопустимая.

Показатель корректности функционирования СЗИ НСД ($Е_{кф}$) вычисляется на основе моделирования динамики функционирования СЗИ НСД в АС как системы массового обслуживания. Динамика функционирования СЗИ НСД формально представляется с помощью аппарата Е-сети. В основе корректности функционирования СЗИ НСД лежит время реализации СЗИ НСД защитных функций, поэтому показатель корректности функционирования СЗИ НСД, в соответствии с [2,3], предлагается определять следующим образом:

$$Е_{кф} = P\left(\tau_{кф} \le \tau_{max\ кф}\right), \quad (1)$$

где $\tau_{кф}$ — время реализации СЗИ НСД защитных функций; $\tau_{max\ кф}$ — его максимально допустимое значение.

Показатель корректности функционирования СЗИ НСД оценивается при помощи количественной шкалы, предполагающей оценку в виде действительного числа [0, 1].

Для оценки показателя корректности функционирования СЗИ НСД как объектов контроля по формуле (1) используется полумарковская модель, формируемая на основе Е-сетевого представления динамики функционирования СЗИ НСД [2,3]. Модель динамики функционирования СЗИ НСД для оценки показателя корректности ее функционирования $E_{кф}$ в интересах комплексной оценки эффективности СЗИ НСД и организации автоматизированного контроля эффективности этих систем в АС представляется КПП, вход в начальное состояние которого соответствует обращению к СЗИ, а вход в конечное состояние — окончанию реализации СЗИ своих функций по данному обращению. Основной задачей анализа КПП является вычисление интервально-переходных вероятностей процесса [4].

Конечный полумарковский процесс, моделирующий динамику функционирования ПСЗИ для оценки показателя корректности функционирования, характеризуется полумарковской матрицей

$$H_{кф}(\tau) = \left\| H_{кф\ ij}(\tau) \right\|,\ i = \overline{1,n},\ j = \overline{1,n}. \qquad (2)$$

Произвольный элемент $H_{кф\ ij}(\tau)$ этой матрицы есть вероятность того, что соответствующий КПП, оказавшись в состоянии i, перейдет из него непосредственно в состояние j, причем за время, меньшее τ, и определяется следующим образом:

$$H_{кф\ ij}(\tau) = p_{кф\ ij}\ G_{кф\ i}(\tau),\ i = \overline{1,n},\ j = \overline{1,n}, \qquad (3)$$

где $p_{кф\ ij}$ — вероятности перехода КПП из состояния i непосредственно в состояние j при условии, что этот КПП оказался в состоянии i; $G_{кф\ i}(\tau)$ — функции распределения времени пребывания КПП в состоянии i.

Переходные вероятности $p_{кф\ ij},\ i = \overline{1,n},\ j = \overline{1,n}$ определяются разрешающими процедурами, а функции распределения $G_{кф\ i}(\tau),\ i = \overline{1,n}$ — процедурами временной задержки соответствующих переходов Е-сети, формализующей динамику функционирования СЗИ. Законы распределения для функций $G_{кф\ i}(\tau)$ предполагаются известными при комплексной оценке эффективности СЗИ в АС. Однако их параметры и переходные вероятности $p_{кф\ ij}$ не могут быть заранее достоверно и навсегда определены. Поэтому предполагаются заранее известными лишь их предварительные значения. Для корректировки этих значений используются результаты статистической обработки данных о параметрах выполнения СЗИ НСД своих функций ЗИ при реализации сервисных задач в АС.

Показатель корректности функционирования СЗИ НСД, отражающий ВВХ динамики функционирования системы, определяется как вероятность своевременного достижения КПП конечного состояния. Исходя из этого, основой для исследования ВВХ динамики функционирования СЗИ НСД является система уравнений полных вероятностей перехода из состояний КПП, моделирующего динамику функционирования СЗИ НСД, в его конечное состояние, за время меньшее τ, сформированная на основе анализа системы уравнений интервально-переходных вероятностей КПП [4]:

$$Q_{кф\ i}(\tau) = p_{кф\ in} \cdot G_{кф\ i}(\tau) + \sum_{j=1}^{n-1} p_{кф\ ij} \cdot G_{кф\ i}(\tau) * Q_{кф\ j}(\tau),\quad i = \overline{1,n-1}, \qquad (4)$$

где $Q_{кф\ i}(\tau)$ — вероятность того, что КПП из состояния i достигнет конечного состояния n, причем за время, меньшее τ.

Данная система уравнений связывает ВВХ отдельных состояний КПП (состояний функционирования СЗИ НСД) с ВВХ КПП в целом (динамики функционирования СЗИ в целом).

Для упрощения системы интегральных уравнений (4) используем преобразование Лапласа. В результате получим систему алгебраических уравнений для производящих функций:

$$q_{\text{кф}\,i}(\nu) = p_{\text{кф}\,in} \cdot g_{\text{кф}\,i}(\nu) + \sum_{j=1}^{n-1} p_{\text{кф}\,ij} \cdot g_{\text{кф}\,i}(\nu) * Q_{\text{кф}\,j}(\nu), \quad i = \overline{1,n-1}, \qquad (5)$$

где $q_{\text{кф}\,i}(\nu)$ — преобразование Лапласа функции $Q_i(\tau)$; $g_{\text{кф}\,i}(\nu)$ — преобразование Лапласа функции $G_i(\tau)$.

При этом преобразование Лапласа элементов полумарковской матрицы $H_{\text{кф}\,ij}(\tau)$ определяется как

$$h_{\text{кф}\,ij}(\nu) = p_{\text{кф}\,ij} \cdot g_{\text{кф}\,i}(\nu). \qquad (6)$$

Величина $g_{\text{кф}\,i}(\nu)$, необходимая для проведения расчетов для типовых распределений времени пребывания СЗИ НСД в состоянии i, определяется следующим образом.

Если время пребывания СЗИ НСД в состоянии i есть равномерно распределенная на отрезке $[a_i;b_i]$ случайная величина, то

$$g_{\hat{e}\hat{o}\,i}(\nu) = \frac{exp(-a_i\nu)[1-exp(-b_i\nu)]}{b_i\nu}. \qquad (7)$$

В случае экспоненциального распределения времени пребывания СЗИ НСД в состоянии i, со средним значением b_i, имеем:

$$g_{\text{кф}\,i}(\nu) = \frac{1}{1+b_i\nu}. \qquad (8)$$

Если время пребывания СЗИ НСД в состоянии i оценивается нормально распределенной случайной величиной со средним значением μ_i и достаточно малой дисперсией σ_i^2, то

$$g_{\hat{e}\hat{o}\,i}(\nu) = exp(-\mu_i\nu + \frac{1}{2}\sigma_i^2\nu^2). \qquad (9)$$

Для удобства записи будем подразумевать:

$h_{ij} = h_{\text{кф}\,ij}(\nu)$; $q_i = q_{\text{кф}\,i}(\nu)$.

Учитывая выражение (6), систему уравнений (5) можно представить в следующем виде:

$$\begin{cases} (1-h_{1,1})q_1 - h_{1,2}q_2 - h_{1,3}q_3 - \ldots - h_{1,n-1}q_{n-1} = h_{1,n}; \\ -h_{2,1}q_1 + (1-h_{2,2})q_2 - h_{2,3}q_3 - \ldots - h_{2,n-1}q_{n-1} = h_{2,n}; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ -h_{n-1,1}q_1 - h_{n-1,2}q_2 - h_{n-1,3}q_3 - \ldots + (1-h_{n-1,n-1})q_{n-1} = h_{n-1,n}. \end{cases} \qquad (10)$$

Для решения этой системы уравнений используем метод исключения Гаусса. Данный метод имеет ограничение: «ведущие» коэффициенты уравнений системы должны быть не равны нулю. Это ограничение для рассматриваемой системы уравнений выполняется, так как $h_{ii} < 1$ для $i = \overline{1,n-1}$ и «ведущие» коэффициенты уравнений системы $(1-h_{ii})$ всегда больше нуля.

Разделив все члены первого уравнения на $(1-h_{11})$, получим

$$q1 - h_{1,2}^{(1)}q2 - h_{1,3}^{(1)}q3 - \ldots - h_{1,n-1}^{(1)}qn\text{-}1 = h_{1,n}^{(1)}, \qquad (11)$$

где $h_{i,j}^{(1)} = \frac{h_{1,j}}{1-h_{1,1}}$, $j = \overline{2,n}$.

Для исключения q_1 из остальных уравнений системы (10) помножим уравнение (11) на соответствующий коэффициент при q_1 ($-h_{i,1}$) в каждом из уравнений системы (10) и полученное уравнение вычтем из i-го уравнения ($i=\overline{2,n-1}$).

Получим следующую систему уравнений:

$$\begin{cases} q_1 - h_{1,2}^{(1)} q_2 - h_{1,3}^{(1)} q_3 - \ldots - h_{1,n-1}^{(1)} q_{n-1} = h_{1,n}^{(1)}; \\ (1 - h_{2,2}^{(1)}) q_2 - h_{2,3}^{(1)} q_3 - \ldots - h_{2,n-1}^{(1)} q_{n-1} = h_{2,n}^{(1)}; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ -h_{n-1,2}^{(1)} q_2 - h_{n-1,3}^{(1)} q_3 - \ldots + (1 - h_{n-1,n-1}^{(1)}) q_{n-1} = h_{n-1,n}^{(1)}. \end{cases} \quad (12)$$

где $$h_{i,j}^{(1)} = h_{i,j} + h_{i,1} h_{1,j}^{(1)}, \quad i=\overline{2,n-1},\ j=\overline{2,n}. \quad (13)$$

Из системы (12) указанным выше приемом исключим неизвестное q_2 и получим новые коэффициенты, которые будут вычисляться по формулам типа (13) и т.д. — прямой ход метода Гаусса.

В результате преобразований получим систему приведенных уравнений:

$$\begin{cases} q_1 - h_{1,2}^{(1)} q_2 - h_{1,3}^{(1)} q_3 - \ldots - h_{1,n-1}^{(1)} q_{n-1} = h_{1,n}^{(1)}; \\ q_2 - h_{2,3}^{(2)} q_3 - \ldots - h_{2,n-1}^{(2)} q_{n-1} = h_{2,n}^{(2)}; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ q_{n-1} = h_{n-1,n}^{(n-1)}. \end{cases} \quad (14)$$

где $$h_{k,j}^{(k)} = \frac{h_{k,j}^{(k-1)}}{1 - h_{k,k}^{(k-1)}}, \qquad h_{i,j}^{(k)} = h_{i,j}^{(k-1)} + h_{i,k}^{(k-1)} h_{k,j}^{(k)}, \qquad h_{ij}^{(0)} = h_{ij}, \quad (15)$$

$$k=\overline{1,n-1},\ \ i=\overline{k+1,n-1},\ \ j=\overline{k+1,n}.$$

Отсюда последовательно находим неизвестные системы уравнений — обратный ход метода Гаусса.

$$\begin{cases} q_{n-1} = h_{n-1,n}^{(n-1)}; \\ q_{n-2} = h_{n-2,n}^{(n-2)} + h_{n-2,n-1}^{(n-2)} q_{n-1}; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ q_1 = h_{1,n}^{(1)} + h_{1,n-1}^{(1)} q_{n-1} + h_{1,n-2}^{(1)} q_{n-2} + \ldots + h_{1,2}^{(1)} q_2. \end{cases} \quad (16)$$

Введем обозначение $\nu_m = \frac{1}{\tau_m}$ — параметр экспоненциального закона распределения максимально допустимого времени реализации защитных функций $\tau_{max\ кф}$. Величина τ_m является средним значением случайной величины $\tau_{max\ кф}$.

Определенный равенством (1) показатель корректности функционирования СЗИ НСД, характеризующий ВВХ динамики функционирования СЗИ НСД, выражается через ВВХ отдельных состояний функционирования СЗИ НСД следующим образом:

$$E_{êô} = q_{êô\ 1}(\nu_m). \quad (17)$$

При вычислении показателя $E_{кф}$ в качестве аргумента ν используется параметр ν_m.

Таким образом, для определения показателя корректности функционирования СЗИ НСД ($E_{кф}$) сначала вычисляются $g_i(\nu_m)$ с помощью формул (7)—(9) или аналогичных им для других законов распределения, затем определяются величины $h_{ij}(\nu_m)$ по формуле (6), далее вычисляются коэффициенты уравнений системы (14) с помощью выражений (15), наконец, искомое значение показателя корректности функционирова-

ния СЗИ НСД ($E_{кф}$), определенного равенством (17), вычисляется с помощью системы уравнений (16) с подстановкой $\nu = \nu_m$.

Большее значение любого показателя интерпретируется как лучшая эффективность СЗИ НСД по данному показателю.

Комплексная оценка эффективности СЗИ НСД как объекта контроля осуществляется с помощью интегрального показателя эффективности СЗИ НСД ($E_{и}$), объединяющего элементарные показатели, рассмотренные выше. Для формирования интегрального показателя эффективности СЗИ НСД проанализируем элементарные показатели.

Качественные показатели $E_{ф}$ и $E_{уи}$ в силу их булевозначности не могут рассматриваться в качестве интегрального показателя, а могут быть только в ограничениях:

$$E_{ф} = 1;\ E_{уи} = 1. \tag{18}$$

Два ограничения можно записать в форме одного ограничения:

$$E_{ф} \wedge E_{уи} = 1. \tag{19}$$

Показатель корректности функционирования СЗИ НСД ($E_{кф}$) предлагается использовать, с одной стороны, также в ограничениях, так как требование к оперативности АС накладывает соответствующее ограничение на функционирование СЗИ НСД:

$$E_{кф} \geq E_{\min кф}, \tag{20}$$

где $E_{\min кф}$ — минимальное значение корректности функционирования СЗИ НСД, заданное разделом «Требования к подсистеме ЗИ от НСД» программной документации на АС, с другой стороны, целесообразно рассматривать как интегральный показатель эффективности СЗИ НСД, так как данный показатель количественно оценивает эффективность выполнения данной системой возложенных на неё защитных функций (своевременность реализации СЗИ НСД этих функций). Исходя из этого, выражение для оценки интегрального показателя эффективности СЗИ можно записать в следующем виде:

$$E_{è} = \begin{cases} E_{êô}, & åñëè \ \left(E_{êô} \geq E_{min\,êô}\right) \wedge E_{ô} \wedge E_{óè} = 1, \\ 0, & åñëè \ èíà÷å. \end{cases} \tag{21}$$

Таким образом, комплексная оценка эффективности СЗИ НСД приравнивается к оценке показателя корректности функционирования СЗИ НСД при условии, что величина показателя $E_{кф}$ не меньше заданной $E_{\min кф}$ и остальные элементарные показатели «допустимы».

ЛИТЕРАТУРА

1. Скрыль С.В., Вохминцев В.А. Математическое моделирование как инструмент исследования процессов защиты информации в деятельности органов внутренних дел // Современные проблемы борьбы с преступностью: материалы Всероссийской научно-практической конференции (информационная безопасность). — Воронеж: Воронежский институт МВД России, 2005. — С. 14—15.

2. Окрачков А.А. Модели и алгоритмы автоматизированного контроля эффективности программных систем защиты информации: автореф. дис. … канд. техн. наук. — Воронеж, 2008.

3. Модели и алгоритмы автоматизированного контроля эффективности систем защиты информации в автоматизированных системах: монография / А.А.Окрачков [и др.]. — Воронеж: Воронежский институт МВД России, 2012.

4. Тихонов В.И., Миронов М.А. Марковские процессы. — М.: Сов. радио, 1977.